EDUCATE INFORM CONNECT

2011-2012

CATALOG

Message from the Chancellor

On December 1, 2010, I was proud to represent the NDU iCollege, along with NDU President, Vice Admiral Ann E. Rondeau, USN, as we brought to a close the 3-year degree-granting process at the U.S. Department of Education. The 18-member National Advisory Committee for Institutional Quality and Integrity (NACIQI) and the Department of Education unanimously recommended that the NDU iCollege be awarded degree-granting authority and that the current class be eligible to receive degrees once they complete educational requirements. The NDU iCollege's first Government Information Leadership Master of Science Degree recipients were awarded their degrees at the NDU graduation ceremony in June 2011. The college is now accepting applications from potential students who wish to enter our Master's Program. This is a great accomplishment for our faculty and staff!

In addition to our new Master's Degree, the NDU iCollege will be offering four new graduate certificate programs this Fall – Chief Technology Officer (CTO), Cyber-Leadership (Cyber-L), Information Operations (IO), and Information Technology Program Management (ITPgM). The CTO Certificate will focus on emerging technologies, assessing current markets, examining external business relationships, and ensuring transparency and information security. The new Cyber-L Certificate will emphasize overcoming information overload while leveraging cyberspace advantages through the creation of strategies, policies, understanding law, and management of information technology. The IO Certificate will prepare future strategic leaders to effectively integrate and employ the information component of national power in the development and execution of national military and security strategies. The ITPgM Certificate is designed to meet the ever-increasing call for program managers across the federal government. Finally, the college's very popular Information Assurance Program (5 certificates) will be re-named Cyber Security (Cyber-S).

As we begin the 2012 academic year, I am very pleased to reflect on the accomplishments of our faculty, staff, and students. In working to achieve our vision to become "the global hub for educating, informing, and connecting Information Age leaders," the college has been on the forefront of critical global activities. International conferences have included "Regional Collaboration in Cyber Security" (July 2010, Singapore) with The Honorable Jaak Aaviksoo, Minister of Defense in Estonia, as the keynote speaker; "Cloud Computing" (Oct 2010, London), with John Suffolk, UK CIO, as the keynote; and "Critical Information Infrastructure Protection" (Feb 2011, Dubai) with His Highness Sheikh Nahayan, UAE Minister of Higher Education, as the guest of honor and evening dinner keynote. We are currently planning our next overseas event, the "2nd Annual Cyber Conference" (Sept 2011, Bangkok). These exciting global conferences allow the NDU iCollege the opportunity to educate information leaders worldwide, continue government and public/private partnerships, and help build awareness of the National Defense University's colleges, components, and programs.

Closer to home, the college held a "Social Media Conference" at NDU in November 2010, with General James E. Cartwright, Vice Chairman of the Joint Chiefs of Staff, as our keynote speaker. Also in November, in conjunction with the CFO Council, we hosted the 20th Anniversary of the CFO Act. The college continues to lead the Federal Consortium for Virtual Worlds (FCVW), including hosting the annual FCVW Expo each May at Fort McNair. From a small group of 40 federal employees, the Consortium now has over 2,200 members across the U.S. government and private sector who share ideas and best practices for working together to achieve the missions of their organizations by using virtual worlds' technologies.

The upcoming academic year will bring several inspirational changes to the NDU iCollege. Our new Ci Center will exhibit "workplace of the future" technologies and be used by faculty and staff in innovative ways to deliver courses and services (expected completion, Fall 2011). We will also be moving the college's leadership team to the 2nd Floor of Marshall Hall to allow for faculty and student meeting spaces, new faculty offices, and space on the 1st floor for new classrooms. Finally, we will complete a major overhaul of the college's website to provide quicker, easier access to course information and scheduling, application instructions, news items, and information on how to register for events.

We look forward to seeing you this year at the NDU iCollege!

Robert D. Childs
Chancellor, NDU iCollege

Contents

MISSION:

Prepare military and civilian leaders to direct the information component of national power by leveraging information and information technology for strategic advantage.

Overview

Professor Gilliam Duvall, Chair, Cyber Integration and Information Operations Department teaches a class in the NDU iCollege telepresence room

The NDU iCollege Experience

The NDU iCollege offers a wide spectrum of educational activities, services, and programs to prepare information leaders to play critical roles in national security in the Information Age. In every course, program, and workshop, students with diverse perspectives contribute to a rich and dynamic learning environment. They are motivated to learn and share knowledge, experience, and best practices. Our students are encouraged to become better leaders and decision-makers and to master the tools of lifelong learning. Students, graduates, employers, leaders, and practitioners create a global learning community to foster innovation and creativity.

Strategic Leader Development for You and Your Organization

In December 2010, the National Advisory Committee for Institutional Quality and Integrity (NACIQI) and the Department of Education unanimously recommended that the NDU iCollege be awarded degree-granting authority for the Government Information Leadership (GIL) Master of Science Degree. The GIL M.S. degree has a core of management, leadership, and information technology courses focused on the unique challenges and opportunities of defense and government. Students pursuing the M.S. degree select one of nine areas of concentrations that align with the NDU iCollege certificates. In addition to graduate-level courses, the NDU iCollege offers all courses for professional development and welcomes students to enroll without seeking a certificate or academic credit. A third option for strategic leader development is "education in context." These educational opportunities include workshops, presentations, seminars, and events to develop the workforce to meet the needs of government to accomplish assigned missions and to develop leaders who can leverage the information component for national security.

Learning That Is Current, Relevant, and Future-Focused

Our faculty offer innovative curricula focused on relevant questions, challenges, and opportunities facing today's defense and government leaders. While challenging students to develop their competencies in strategic thinking, focus on the enterprise, collaboration and cross-boundary leadership, leveraging resources, and executive values and skills, the faculty guide students through interactive instruction, including case studies, problem-based learning, field studies, and simulations. These activities are supplemented by a

variety of guest speakers, leaders and experts who contribute unique perspectives and experiences to the learning environment.

Access to Learning Wherever You Are

To respond to the needs of its learning community, the NDU iCollege offers students opportunities and tools for face-to-face interaction and e-learning supported by online library resources and course management software. Classrooms on campus at Fort Lesley J. McNair in Washington, D.C., are equipped with computers for student use during eResident courses. Blackboard (Bb) supports the virtual classroom environment for all students and faculty around the world. Online library resources are available via web access through the Student Resources Portal in Bb where students can access the library as long as they are students at the NDU iCollege. The College regularly pilots new technologies to enhance the teaching and learning process and provides students and their organizations with flexible learning options to accommodate their location, work schedule, and learning preferences

Intensive courses are offered either through a blended model or by distributed learning (DL) for students around the globe.

eResident Format

The eResident format (see figure below) uses a blended model in which students and faculty engage in both online and resident activities that ensure high quality interaction and feedback, student learning and assessment, and academic rigor. Each offering of five (5) weeks consists of four (4) components: PREPARATION, SEMINAR, SYNTHESIS, and ASSESSMENT

Preparation

The first week of an eResident course is an asynchronous DL lesson designed to prepare students for the face-to-face component of the course that begins in the second week. Students begin by signing in to Blackboard (Bb), retrieving their readings, assignments, and other course instructions. During this PREPARATION week of virtual engagement, students must complete the assigned readings, participate online in activities, and complete the assignments due no later than NOON on FRIDAY. The faculty leading the course offering will assign a grade of "W" (Withdrawl) to students who do not sign into Blackboard and satisfactorily engage in the required activities during the PREPARATION week (i.e., a grade of "W" will drop the student from the course on Friday afternoon.) Students who receive a "W" may not attend the SEMINAR (resident) portion the following week. Students seeking credit or a Professional Development (PD) grade must meet the requirements of the PREPARATION week.

Seminar

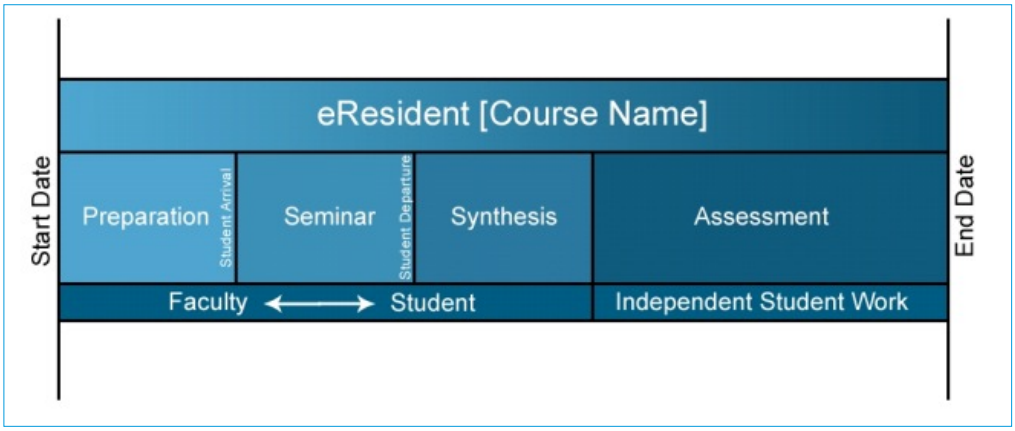
Immediately following the one-week PREPARATION DL lesson, students attend a five-day in-residence SEMINAR. During this full-time week of SEMINAR, students and faculty participate in an interactive learning environment in NDU iCollege classrooms at Ft. McNair (or other designated location). The SEMINAR is conducted from 8 to 5 Monday through Friday, with homework often assigned to prepare for the next day's lessons.

Synthesis

In the week immediately following the SEMINAR, students and faculty engage virtually in a one-week asynchronous DL lesson designed to synthesize learning and prepare students for the follow-on graded final assessment. Participation in SYNTHESIS is required and graded for student seeking credit for the course, but is optional for students seeking a Professional Development (PD) grade.

Assessment

Students enrolled for certificate/graduate credit must complete an end-of-course ASSESSMENT, typically a substantive paper or project. Students may engage



virtually with the faculty and/or other students as appropriate. Normally, assessments are due no later than the Monday, 2 ½ weeks after the last day of the SYNTHESIS (as noted as the last day of the course offering in the schedule).

The Distributed Learning (DL) Format

The Distributed Learning (DL) format engages students and faculty virtually in preparation, seminar, synthesis, and assessment over 12 weeks via Bb. Students enrolled for certificate/graduate credit must complete an end-of-course assessment typically consisting of a substantive paper or project that allows students to demonstrate their mastery of the intended learning outcomes. To receive credit for a course, students must be actively engaged virtually in every DL lesson as assigned by faculty. Assessments are due no later than the Monday following the 12th week, as specified in the schedule of course offerings. See the NDU iCollege Schedule of Course Offerings for beginning and ending dates of courses.

Advanced Management Program (AMP)

AMP is a 14-week resident program conducted at Fort McNair in Washington, D.C twice a year that leads to the Chief Information Officer (CIO) Certificate, Cyber Leadership (Cyber-L) Certificate, Chief Financial Officer (CFO) Leadership Certificate, or the Government Strategic Leader (GSL) Certificate. Students begin the program two weeks prior to arriving at Ft. McNair. They sign in to Blackboard, obtain their readings, assignments, and other course instructions. During that time, students complete assigned readings, participate virtually in course activities, and prepare the assignments due when they start the 14-week resident portion of the AMP.

Other Formats

Elective courses are offered for in-residence students attending National War College, Industrial College of the Armed Forces, and the College of International Security Affairs' students in residence at Fort McNair.

Seminars, symposia, workshops, and other educational activities are conducted by faculty to meet particular learning needs of organizations on specific issues and topics.

Emerging Leader Workshops address the needs of future leaders and those who want to advance to the next level of their careers. Geared toward GS-9s to GS-11s or equivalents, the workshops provide foundational education in the issues, challenges, and competencies of information leaders.

AMP 42 students at the City of New York Police Department during domestic travel

The College at a Glance

The Chancellor of the NDU iCollege provides strategic direction and vision for all faculty, staff, and students, while the Dean of Faculty and Academic Programs oversees faculty, curriculum, and instruction. The Dean of Students and Administration oversees operational support for the College. The following three academic departments and one Academy conduct the College's educational programs:

Information Strategies Department (IS)

The IS Department focuses on policy and planning processes, leadership and management competencies, and perspectives for information resources management that form the foundation of the College's Chief Information Officer (CIO) Certificate Program. Consistent with the Clinger-Cohen Act (CCA) of 1996, the department delivers CCA-related core courses and works closely with other departments to prepare graduates for leadership positions in the offices of CIOs across DOD and the Federal Government. In addition to the CIO Certificate, the Information Strategies Department also delivers the GSL Certificate and its concentration in the M.S. Degree Program.

2011 NDU iCollege leadership team, faculty and staff group photo

The Cyber Integration and Information Operations Department (CI&IO)

The CI&IO Department focuses on information operations, assurance, and security in the planning and execution of national and military strategy. The Cyber Security (Cyber-S) Certificate Program consists of nested certificates that emphasize cyber security issues and fundamental approaches to the protection of the nation's information infrastructure. These certificates include: National Training Standard for Information Systems Security Professionals (NSTISSI No. 4011), National Information Assurance Training Standard for Senior Managers (CNSSI No. 4012), National Information Assurance Training Standard for System Security Certifiers (NSTISSI 4015), National Information Assurance Training Standard for Risk Analysts (CNSSI 4016), and the Chief Information Security Officer (CISO) Certificate. The Department also sponsors the Information Operations and Cyber Leadership (Cyber-L) Certificates and their concentrations in the M.S. Degree Program.

The Systems and Technology Department (S&T)

The S&T Department delivers courses and programs focused on successful application of project and program management leadership skills, policies, best practices, and tools to acquire and manage an enterprise's information systems, software, and services. Its courses examine IT project and program management, acquisition, enterprise architecture strategies, business case development, and data management strategies. The Systems and Technology Department delivers the Chief Technology Officer (CTO), Enterprise Architecture (EA), IT Project Management (ITPM)*, and IT Program Management (ITPgM) Certificates and their concentrations in the M.S. Degree Program.
* ITPM is not offered as an M.S. concentration.

Chief Financial Officer Academy (CFO)

The CFO Academy is sponsored by the DOD Comptroller and endorsed by the Federal CFO Council. The Academy offers graduate-level courses and educational services for middle- to senior-level personnel in the government financial management community to prepare them to create and lead 21st Century government organizations. The CFO Academy sponsors the CFO Leadership Certificate and its concentration in the M.S. Degree Program.

National Center of Academic Excellence in Information

The NDU iCollege is a National Center of Academic Excellence (CAE) in Information Assurance Education as certified by the National Security Agency and the Department of Homeland Security. The College was

originally certified in the year 2000 and subsequently re-certified three times. The College established the Center for Information Assurance Education to conduct education and research focused on concepts and best practices related to information assurance for national security. In its leadership role in information assurance strategies, the Center facilitates understanding of the status and practices of information assurance, and conducts and disseminates research on information security, information operations, homeland security, and Critical Information Infrastructure Protection

Joint Professional Military Education (JPME)

The NDU iCollege provides instruction as a component of the Joint Professional Military Education (JPME) taught by the Industrial College of the Armed Forces (ICAF) and the National War College (NWC). The Information Operations Concentration, open to select students of ICAF and NWC, consists of three required electives focused on the use of information in the planning and execution of national strategy, military strategy, and joint operations. Additionally, other students from ICAF and NWC may attend up to four elective courses at the NDU iCollege during their academic year.

Professional Development Opportunities

Professional Development Grade

The NDU iCollege offers all courses for either graduate/certificate credit or Professional Development (non-credit). The College welcomes students who wish to enroll in individual courses to learn and to connect with others without seeking a certificate or academic credit. In such cases, students will receive a grade of Professional Development (PD) in their academic records and on their official NDU transcripts. (Refer to the section on Grading for more information.) Students enrolled in certificate programs may take courses for a PD grade; however, for courses to count toward a certificate, the Master's Degree, or as a prerequisite, students must take them for credit.

Students electing courses for professional development will:

- Discuss their intent to take a course for professional development with each Offering Leader, and
- Satisfy attendance and participation requirements for the course as outlined in its assessment plan.

Professional Development Enrollment

Students undecided on which certificate program best suits their needs may enroll in the College as Professional Development students. Professional Development students may take courses for either graduate/certificate credit (academic credit) or professional development (non-credit). Students may transfer an unlimited number of courses taken while in a Professional Development student status toward a certificate requirement at any time, as long as the course was taken for academic credit (not a PD grade). This will allow undecided students to sample courses before applying to a certificate program.

If you are not already in a certificate program, you may enroll in the NDU iCollege as a Professional Development student through the NDU iCollege website (http://www.ndu.edu/icollege).

Why You Might Choose a Course for Professional Development

- You are looking for courses designed to enhance your ability to perform your job more efficiently and effectively.
- You completed a certificate with the iCollege and/or have an advanced degree and are now focused on specific tasks or duties that require additional knowledge or perspectives.
- You are an information leader who wants to refresh your knowledge by taking new courses.
- You are new to the iCollege and interested in trying out the courses before you commit to a certificate program.
- Your career field requires you to take continuing education courses to satisfy or maintain certifications. Talk with your personnel office to ensure you are enrolling in the correct courses.

National Security Professional Development (NSPD)

The NDU iCollege has been an early and active partner in support of Executive Order 13434, National Security Professional Development (NSPD) (May 17, 2007). The NDU iCollege faculty contributed as members of the initial working groups addressing topics such as competencies, curriculum, and professional experience. The College offers a wide range of courses designed to develop and strengthen desired National Security Professionals shared capabilities. As the NSPD program matures, the College remains at the forefront in educating future National Security Professionals in the identified competencies through our course offerings.

NDU iCollege iLabs

The National Defense University (NDU) iCollege educates mid-to-senior information leaders in a variety of IT-related competencies (Chief Information Officer, Chief Technology Officer, Cyber, etc.). One of the key problems for today's government leaders is they don't have the time or resources to procure the latest technologies, learn the vulnerabilities of those technologies, and determine the best ways to use IT in the workplace.

Dr Childs in the Innovations and Simulations Lab

The NDU iCollege's computer laboratories ("iLabs") help solve this vital issue by providing hands-on learning and research opportunities for U.S. Federal Government, private sector, and international students. iLab participants experience technology-rich learning to enhance knowledge transfer and to keep the U.S. Government and its partners ahead of the steeply accelerated technology curve. Additionally, the iLabs provide insight and training through flexible and mobile workshops and symposia across the globe.

"Currency" is always a challenge with rapidly-changing technologies, so the college has created strong partnerships with corporations like Microsoft, Google, IBM, Cisco, Tibco, McAfee, and others, to bring the latest tools and technologies into the labs and to assure key components can be taken on the road for global education and training purposes.

Research and Experiential Learning

- Supervisory Control and Data Acquisition (SCADA)/Control System: Promote awareness in the protection of electrical, oil, gas, water, and transportation systems.
- Cyber Attack and Defense: Provide a hands-on introduction to tools and techniques used by hackers to compromise computer networks and methods for mitigating the attacks.
- Firewalls and Intrusion Detection Systems: Halt the ingress or egress of communications based upon an address of origination or destination, port access, protocol access, or application program access.
- Biometrics: Hands-on experience using devices including fingerprint scanners, voice identification equipment, face print identification, hand geometry identifiers, and iris scanners.
- Wireless Security: Methods for breaking simple wireless encryption schemes as well as proper methods for locking down unauthorized access.
- Digital Forensics: Hands-on learning methods for identifying, screening, and securing organizational policy infractions and cyber crime incidents.
- Voice over Internet Protocol (VOIP) and Radio Frequency Identification (RFID): Witness the vulnerabilities and safeguards associated with using computer networks for voice traffic and RFID.
- CyberProtect Network Defense Simulation: Play the role of a system protector to discover points of exploitation and apply appropriate countermeasures.
- Crisis Management: Witness high-end audio and video infrastructure capable of displaying multiple real-time, simulated, or a real-time/simulated mix of data feeds designed to simulate crisis scenarios.
- Virtual Worlds: Supporting the NDU iCollege lead of the Federal Consortium for Virtual Worlds, the iLabs host 3D virtual environments for government leaders to teach, learn, research, experiment and collaborate.
- Gaming and Simulations: Enable individuals, groups, or distributed asynchronous and synchronous gaming and simulation events. Provides both physical and virtual spaces.
- Telepresence: Employs high definition video and audio system capable of connecting professors, students, and guest speakers across the globe for course lectures and international partnership meetings.
- Interactive Pixel: Allows multiple users to import live feeds, presentations, and various tools into one educational session or presentation using a large, interactive touch screen.
- Ci Center: Designed to allow faculty members to use movable classroom furniture and the latest touch screens and other IT tools for a new learning experience every time! Opening Fall 2011

Degree Program

Master of Science in Government Information Leadership (GIL)

The Master of Science in Government Information Leadership (GIL) Degree Program is a selective program that addresses the educational needs of defense and government leaders who seek to lead complex and diverse 21st Century organizations. Participants from across defense and other federal, state, and local government organizations create a learning community hallmarked by partnerships, information sharing, and network synergies.

Goals of the Degree Program
Successful graduates of the Master of Science in Government Information Leadership will be able to:

- Employ information and information technology for strategic advantage
- Evaluate the role, challenges, and opportunities of their organizations within the context of cyber, homeland, national, and global security
- Apply critical, strategic, and innovative thinking to achieve results-oriented organizational goals
- Collaborate across boundaries to leverage talent, resources, and opportunities to achieve mission outcomes and stretch vision
- Create resilient, adaptable, agile, and productive government organizations focused on national security in the Information Age
- Lead Information Age government organizations
- Commit to lifelong development of self and others as reflective learners

Curriculum and Degree Concentrations
The 39 credit curriculum of the GIL Degree offers a combination of information management, technology, and leadership intensive courses in a collaborative and interactive environment. Students select one of nine concentration areas, which correspond to the College's certificate programs, at the time of admission. Concentration areas include: Chief Financial Officer Leadership (CFO), Chief Information Officer (CIO), Chief Technology Officer (CTO), Cyber Leadership (Cyber-L), Cyber Security (Cyber-S), Enterprise Architecture (EA), Government Strategic Leader (GSL), Information Operations (IO), and Information Technology Program Management (ITPgM).

A complete listing of Master of Science concentration descriptions and courses can be found under the heading *Certificate Programs and Degree Concentrations* which immediately follows this section. For current offerings, students should consult the NDU iCollege schedule of classes which can be accessed from the NDU iCollege website at http://www.ndu.edu/icollege. All coursework applied toward a M.S. degree must be completed within the previous seven years.

Cornerstone Seminar

Admitted Master of Science students will be automatically registered in, and must successfully complete, an online not-for-credit cornerstone seminar within six credits of program admission. The cornerstone seminar helps students develop the critical thinking, information technology, communication, and collaboration skills necessary for success in iCollege courses and in their careers as government information leaders. Students research a current issue in their concentration and develop clear and cogent positions in both academic and executive level formats.

Capstone Course

Master of Science students register for the GIL Capstone (CAP) Course as the final course for degree completion. While enrolled in CAP, students complete a capstone synthesis project in his or her area of concentration.

Admission and Degree Requirements
Subject to graduation time limit requirements, a student may use all NDU iCollege classes passed with a grade of B or better toward attaining the M.S. degree. No courses from other institutions are accepted for transfer. Courses taken for Professional Development (PD) are not eligible.

Required Admission Documents
The Government Information Leadership (GIL) Master of Science Degree is a selective degree program. Applicants must include all of the required documents in the same application packet to the NDU iCollege Office of Student Services to be considered for admission.

NDU iCollege Office of Student Services
300 5th Avenue, Marshall Hall
Fort McNair, Washington, DC 20319

1. **Application for Admission** This form includes the applicant's contact information, employer information, and educational background. An applicant must select an admission term and area of concentration. Application forms can be downloaded at http://www.ndu.edu/icollege/pcs/pcs_gil_masters.html

2. **Résumé** A résumé (maximum 3 pages) should include the work history that describes the applicant's position title, organization, responsibilities, and accomplishments, and any awards or recognitions earned. If there are gaps in the résumé, a short paragraph is required to explain them.

3. **Employer Verification and Sponsorship Form** The Employer Verification and Sponsorship Form is used to verify employment. A template can be found on the NDU iCollege website at http://www.ndu.edu/icollege/admis_appover5.htm. The form must be printed on organizational letterhead. The applicant may also attach additional comments in support of his/her application. The applicant's most immediate supervisor or Human Resources Officer holding a grade of GS/GM-12, O-4, or higher, must complete the form.

4. **One supervisory letter of recommendation and one professional letter of recommendation** Recommendations should be completed on either the recommendation form provided on the NDU iCollege website (http://www.ndu.edu/icollege/admis_appover5.htm) or on organizational letterhead. All recommendations, regardless of format, must address the questions asked on the form. At least one recommendation must come from an individual in the applicant's professional supervisory chain. The second may come from another professional source. Both recommendations should be written by persons able to judge the applicant's ability to complete a challenging graduate-level degree program. Letters of recommendations must be included in the application packet in sealed envelopes.

5. **Official Transcript(s)** Applicants must submit official transcripts from an accredited Bachelor's Degree granting institution and all graduate institutions where graduate work was earned or attempted (regardless of whether credit or degree was issued). The minimum grade point average (GPA) considered for admission is a 3.0 on a 4.0 scale for all previous undergraduate work. In cases where the undergraduate GPA is below a 3.0, a GPA of 3.5 in 12 or more graduate credit hours (from NDU iCollege or other graduate courses) may be used to determine eligibility. Transcripts must bear the official seal of the issuing institution and must be included in the same envelope with all other admissions documents. Do not send transcripts separately to the NDU iCollege Office of Student Services.

Certificate Programs and Degree Concentrations

Chief Financial Officer (CFO) Leadership Program

Administrating Department: Chief Financial Officer Academy
Department Chair: Dr. Todd Holmes

The U.S. Chief Financial Officer (CFO) Council, in conjunction with the DOD Comptroller, launched the CFO Academy in the summer of 2008 at the NDU iCollege. The CFO Academy offers graduate-level courses and services for middle- to senior-level personnel in the government financial management community to prepare them to create and lead 21st Century government organizations.

The primary educational programs offered by the CFO Academy are the CFO Leadership Certificate and the CFO concentration in the Government Information Leadership Master of Science degree program. The CFO Leadership program is noted for a strategic leadership curriculum that is dynamic and relevant to the evolving needs of the government financial management community, including personnel who work in accounting and finance, budget formulation and execution, cost analysis, auditing, and resource management. It focuses on current and future challenges and opportunities facing government, best practices, and strategies of financial management, and the changing role of CFOs as organizational leaders of 21st century government.

Graduates of the CFO Leadership Certificate will be able to:

- Lead within and across organizational boundaries by leveraging information, information technology, human, and financial resources for strategic advantage;
- Balance continuity and change in the development, implementation, and evaluation of financial management strategies, policies, and financial systems while meeting legislative and executive mandates;
- Lead at the enterprise level by linking critical decisions regarding resources, people, processes, and technologies to mission performance, information assurance, and financial systems security requirements;
- Commit to lifelong learning and leadership development of self and others;
- Synthesize theory and best practices from government, private sector, and not-for-profits to achieve the organization's mission; and
- Network with defense, federal, international, and private industry partners.

Vice Admiral Ann Rondeau, President of the National Defense University, speaks to the NDU iCollege graduating class on April 29, 2011

CFO Leadership Certificate
8 Courses Required

Key Competency	Course	Course Title
Core (3)		
	CFF	The Changing World of the CFO
	FFR	The Future of Federal Financial Information Sharing
	RIA	Risk Management, Internal Controls and Auditing for Leaders
Strategic Finance (1)		
	BCP	Budgeting and Congressional Relations for Strategic Leaders
	PFM	Capital Panning and Portfolio Management
Elective (4)		
	AII	Information Assurance and Critical Information Infrastructure Protection
	ARC	Enterprise Architecture for Leaders
	BBC	Building an IT Business Case
	COO	Continuity of Operations
	DMG	Decision Making for Government Leaders
	DMS	Data Management Strategies and Technologies
	ESP	Enterprise Strategic Planning
	IPL	Information Technology Program Leadership
	ITP	Information Technology Project Management
	LCW	Leading the 21st Century Workforce
	LDC -or - SLP	Leadership in the Information Age Strategic Leader Theory and Practice (AMP Students Only)
	MAC	Multi-Agency Information Enabled Collaboration
	MOP	Measuring Results of Organizational Performance
	OCL	Organizational Culture for Strategic Leaders
	PRI	Strategies for Process Improvement
	WGV	Web Enabled Government

Dr. Todd Holmes, Chair, CFO Academy

Government Information Leadership (GIL) MS Degree
Chief Financial Officer (CFO) Concentration
13 Courses Required

	Course	Course Title
Foundational (3)		
	GLS	Global Strategic Landscape
	OCL	Organizational Culture for Strategic Leaders
	CAP	Capstone Course
Leadership (2)		
	AII	Information Assurance and Critical Information Infrastructure Protection
	ARC	Enterprise Architecture for Leaders
	BBC	Building an IT Business Case
	DMG	Decision Making for Government Leaders
	IPL	Information Technology Program Leadership
	LCW	Leading the 21st Century Workforce
	LDC -or - SLP	Leadership in the Information Age Strategic Leader Theory and Practice (AMP Students Only)
	MAC	Multi-Agency Information Enabled Collaboration
Management (2)		
	COO	Continuity of Operations
	ESP	Enterprise Strategic Planning
	ITP	Information Technology Project Management
	MOP	Measuring Results of Organizational Performance
	PRI	Strategies for Process Improvement
Technology (1)		
	DMS	Data Management Strategies and Technologies
	WGV	Web Enabled Government
Core (5)		
	BCP	Budgeting and Congressional Relations for Strategic Leaders
	CFF	The Changing World of the CFO
	FFR	The Future of Federal Financial Information Sharing
	PFM	Capital Planing and Portfolio Management
	RIA	Risk Management, Internal Controls and Auditing for Leaders

Chief Information Officer Program (CIO)

Administrating Department: Information Strategies Department
Department Chair: Dr. John T. Christian

The NDU iCollege CIO Program is the recognized leader in graduate education for Federal CIO leaders and agency personnel. It directly aligns with the Federal CIO Council-defined CIO competencies and addresses the Clinger-Cohen Act and other relevant legislation mandates as well as the current administration's interpretations and implementations of these legislative actions. Successful CIO graduates will be able to:

- Lead within and across federal organizational boundaries by leveraging information, information technology, human, and financial resources to link critical decisions regarding resources, people, processes, and technologies to mission performance and information assurance
- Balance continuity and change in the development, implementation, and evaluation of government information resources and management strategies and policies while meeting legislative and executive mandates
- Build viable networks across defense, federal, global, and private sector partners
- Commit to lifelong learning and leadership development of self and others

CIO Program graduates earn a certificate signed by the DOD CIO and the NDU iCollege Chancellor that recognizes they have earned an education in the Federal CIO competencies. The CIO Certificate Program is organized around 13 subject areas directly related to CIO competencies identified by the Federal CIO Council (see the CIO Wheel below). Selected courses allow students to tailor their CIO program of study to meet their organization's needs and priorities. Additionally, the CIO Certificate is a concentration in the Government Information Leadership Master of Science Degree.

Courses in each competency are designated as "core" because of their breadth and necessary links to the CIO competency, or as "elective" because of their depth in a particular competency. Students work with their supervisors and the College's Academic Advisor to tailor their program to fit their professional and/or organizational needs within the guidelines set by the CIO Council. Students earn the CIO Certificate by successfully completing eight (8) courses:

- Three required core courses
- Five additional elective courses from five different competency areas

Students may apply their certificates, equivalent to at least 15 graduate-level credit hours, toward select master's or doctoral degree programs at several partner institutions of higher education. See the Academic Partner page in this catalog or the NDU iCollege website at http://www.ndu.edu/icollege for additional information. CIO Program graduates are also awarded the Federal CIO University Certificate for Executive Competencies.

CIO Certificate
8 Courses Required

Key Competency	Course	Course Title
Core (3)		
Policy	CIO -or- PRM	CIO 2.0 Roles and Responsibilities Policy Foundations of Information Resources Management (AMP Students Only)
Performance Assessment	MOP	Measuring Results of Organizational Performance
Information Security and Information Management	AII -or- ESS	Information Assurance and Critical Information Infrastructure Protection Enterprise Information Security and Risk Management
Electives (Select 5 Courses, each from a different competency)		
Acquisition	ITA	Strategic Information Technology Acquisition
	SAL	Software Acquisition Leadership
Architecture and Infrastructures	DMS	Data Management Strategies and Technologies
	ARC	Enterprise Architecture for Leaders
Capital Planning and Investment	BBC	Building an IT Business Case
	PFM	Capital Planning and Portfolio Management
eGovernment/eBusiness	WGV	Web Enabled Government
	GIC	Governance in Cyberspace
Leadership	DMG	Decision Making for Government Leaders
	LDC -or - SLP	Leadership in the Information Age Strategic Leader Theory and Practice (AMP Students Only)
Process Improvement	COO	Continuity of Operations
	PRI	Strategies for Process Improvement
Project Management	ITP	Information Technology Project Management
Strategic Planning	ESP	Enterprise Strategic Planning
	IWS	Information, Warfare, and Military Strategy (secret)
Technology Assessment	CST	Critical Information Systems Technologies
	GEN	Global Enterprise Networking
Cyber Security	SPA	Privacy Rights and Civil Liberties
	SEC	Cyber Security for Information Leaders

Special guest commencement speaker, Teresa "Teri" M. Takai, DoD Chief Information Officer, congratulated the NDU iCollege leadership, faculty and staff for creating programs that inspire the information technology community in a continually changing world.

Government Information Leadership (GIL) MS Degree
Chief Information Officer (CIO) Concentration
13 Courses Required

	Course	Course Title
Foundational (3)		
	GLS	Global Strategic Landscape
	OCL	Organizational Culture for Strategic Leaders
	CAP	Capstone Course
Leadership (2)		
Leadership/ Management	DMG -or- LCW -or- LDC -or- SLP	Decision Making for Government Leaders -or- Leading the 21st Century Workforce -or- Leadership in the Information Age -or- Strategic Leader Theory and Practice (AMP Students Only)
Enterprise Architecture	ARC	Enterprise Architecture for Leaders
Process Change Management	MAC	Multi-Agency Information-Enabled Collaboration
Management (2)		
Process Change Management	COO	Continuity of Operations
	PRI	Strategies for Process Improvement
Information Resources Strategy and Planning	ESP	Enterprise Strategic Planning
IT Project/Program Management	ITP	Information Technology Project Management
Acquisition	ITA	Strategic Information Technology Acquisition
Technology(2)		
eGovernment	GIC	Governance in Cyberspace
	WGV	Web Enabled Government
Enterprise Architecture	DMS	Data Management Strategies and Technologies
Technology Management and Assessment	CST -or- EIT -or- GEN	Critical Information Systems Technologies -or- Emerging Information Technologies -or- Global Enterprise Networking
General Technology	CIP	Critical Information Infrastructure Protection
Core (4)		
Policy and Organization	CIO -or- PRM	CIO 2.0 Roles and Responsibilities (Required) Policy Foundations of Information Resources Management (AMP Students Only)
IT Assessment	MOP	Measuring Results Organizational Performance (Required)
Information Security and Information Assurance	AII -or- ESS	Information Assurance and Critical Information Infrastructure Protection (Required) -or- Enterprise Security and Risk Management (Required)
Capital Planning and Investment Control	BBC -or- PFM	Building an IT Business Case - or - Capital Planning Portfolio Management
Cyber Security	SEC -or- SPA	Cyber Security for Information Leaders -or- Privacy Rights and Civil Liberties

Chief Technology Officer (CTO) Program

Administrating Department: Systems and Technology Department
Department Chair: Mr. Andrew P. Gravatt

The number of Chief Technology Officers (CTOs) is rapidly expanding across the federal government even as the role of the CTO continues to evolve. The initial challenge was to leverage new technologies to increase the efficiency and effectiveness of the organization. This demanded full comprehension of the organization's mission and vision, as well as a thorough understanding of emerging technologies. Through strategic partnerships with key stakeholders, industry, and the marketplace, CTOs are moving beyond improvements to existing business processes and proposing innovative solutions to needs not yet fully realized. They practice strong leadership and management skills that enable them to handle the challenges of acquiring and implementing these new technologies and the resulting changes into the business processes of their agencies. The CTO certificate is designed to educate government CTO leaders and their staffs to effectively assess, acquire, and implement emerging technologies to meet the current needs of their organizations and help shape the future vision.

At the completion of their program, successful CTO graduates will be able to:

- Assess the technological maturity of an organization and adapt emerging technologies to achieve current and future strategic organizational goals that are aligned with cyber security requirements.
- Champion and lead successful technology adoption through improved policy, governance, and technology forecasting.
- Use knowledge of acquisition and organizational communication to forecast, assess and select new technologies for integration into an organizational infrastructure.
- Practice horizon research and technology supply chain assurance to ensure that organizations are positioned for the future.
- Network with defense, federal, international, and private industry partners.

CTO Certificate
8 Courses Required

Key Competency	Course	Course Title
Core (3)		
Policy	CTO	CTO Roles and Responsibilities
Emerging Technologies	EIT	Emerging Technologies
Cyber Security	SEC	Cyber Security for Information Leaders
Electives (Select 5 Courses, each from a different competency)		
Leveraging Technology	WGV	Web Enabled Government
	CST	Critical Information Systems Technologies
Leadership	DMG	Decision Making for Government Leaders
	IPL	Information Technology Program Leadership
	LDC -or SLP	Leadership in the Information Age Strategic Leader Theory and Practice (AMP Students Only)
Future Technologies Forecasting and Assessment	FIT	Technology Forecasting and Agency Adoption
Evolving Infrastructure	ARC	Enterprise Architecture for Leaders
	DMS	Data Management Strategies and Technologies
Acquisition	ITA	Strategic Information Technology Acquisition
	SAL	Software Acquisition Leadership
Capital Planning and Investment	BBC	Building an IT Business Case
	PFM	Capital Planning and Portfolio Management
Project Management	ITP	Information Technology Project Management

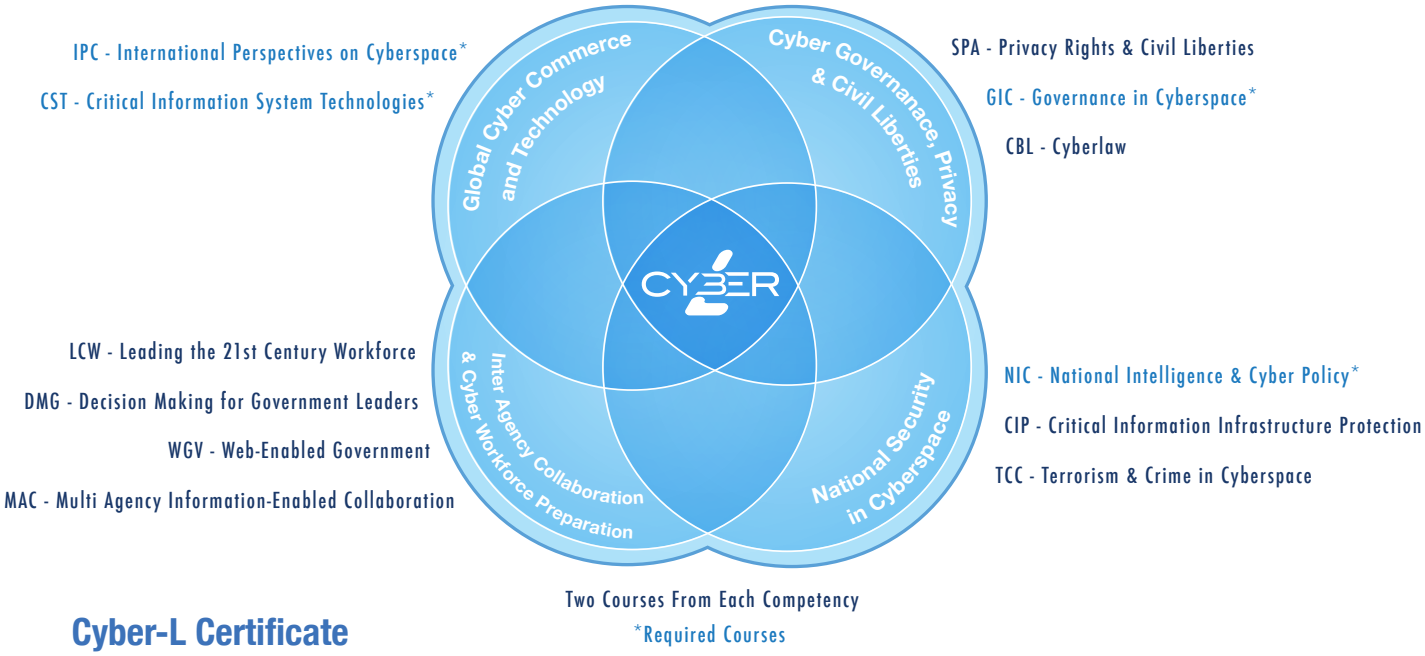
Government Information Leadership (GIL) MS Degree
Chief Technology Officer (CTO) Concentration
13 Courses Required

	Course	Course Title
Foundational (3)		
	GLS	Global Strategic Landscape
	OCL	Organizational Culture for Strategic Leaders
	CAP	Capstone Course
Leadership (2)		
Evolving Infrastructure	ARC	Enterprise Architecture for Leaders (Required)
Leadership	DMG	Decision Making for Government Leaders
	IPL	Information Technology Project Leadership
	LDC -or- SLP	Leadership in the Information Age Strategic Leader Theory and Practice (AMP Students Only)
Management (2)		
Project Management	ITP	Information Technology Project Management
Acquisition	ITA	Strategic Information Technology Acquisition
Technology (3)		
Leveraging Technology	WGV	Web Enabled Government (Required)
Emerging Technology	EIT	Emerging Technologies (Required)
General Technology	DMS	Data Management Strategies and Technologies
	CST	Critical Information Systems Technologies
	GEN	Global Enterprise Networking Telecommunications
	SCS	Managing of Security Control Systems
Core (3)		
Policy	CTO	CTO Roles and Responsibilities (Required)
Cyber Security	SEC	Cyber Security for Information Leaders (Required)
Capital Planning and Investment	BBC	Building an IT Business Case
	PFM	Capital Planning Portfolio Management
Future Technologies Forecasting and Assessment	FIT	Technology Forecasting and Agency Adoption

Cyber Leadership (Cyber-L) Program

Administrating Department: Cyber Integration and Information Operations Department
Department Chair: Mr. Gilliam R. Duvall

The NDU iCollege Cyber Leadership (Cyber-L) program connects secure information sharing and collaboration across U.S. government agencies, the international community, and the private sector. This program develops leadership skills critical to successfully navigate the current cyberspace domain and promote future integration of cyberspace with the physical domains. Multi-disciplinary in nature, Cyber-L is a strategic program that examines the nature of organizations and the people who collaborate using shared information to operate; while securing, protecting, and defending knowledge capital and cyber assets. The curriculum integrates the behavioral, cultural, and national intelligence perspectives with legal, digital forensic, and technology aspects. It examines how leveraging cyberspace advantages can help in creating strategies, policies, and laws that result in improved management of information technology.



Cyber-L Certificate
8 Courses Required

Key Competency	Course	Course Title
Select two courses in each competency		
Cyber Governance, Privacy and Civil Liberties	GIC	Governance in Cyberspace (Required)
	CBL	Cyberlaw
	SPA	Privacy Rights and Civil Liberties
National Security in Cyberspace	NIC	National Intelligence and Cyber Policy (Required)
	CIP	Critical Information Infrastructure Protection
	TCC	Terrorism and Crime in Cyberspace
Inter-Agency Collaboration and Cyber Workforce Protection	DMG	Decision making for Government Leaders
	LCW	Leading the 21st Century Workforce
	MAC	Multi-Agency Information-Enabled Collaboration
	SLP	Strategic Leader Theory and Practice (AMP Students Only)
	WGV	Web Enabled Government
Global Cyber Commerce and Technology	CST	Critical Information Systems Technologies
	IPC	International Perspectives on Cyberspace

Government Information Leadership (GIL) MS Degree
Cyber Leadership (Cyber-L) Concentration
13 Courses Required

	Course	Course Title
Foundational (3)		
	GLS	Global Strategic Landscape
	OCL	Organizational Culture for Strategic Leaders
	CAP	Capstone Course
Leadership (2)		
	DMG	Decision Making for Government Leaders
	LCW	Leading the 21st Century Workforce
	MAC	Multi-Agency Information-Enabled Collaboration
	SLP	Strategic Leader Theory and Practice (AMP Students Only)
Management (2)		
	COO	Continuity of Operations
	TCC	Terrorism and Crime in Cyberspace
Technology (1)		
	CST	Critical Information Systems Technologies
Core (5)		
	GIC	Governance in Cyberspace
	CBL	Cyberlaw
	SPA	Privacy Rights and Civil Liberties
	CIP	Critical Information Infrastructure Protection
	IPC	International Perspectives on Cyberspace
	NIC	National Intelligence and Cyber Policy (Required)

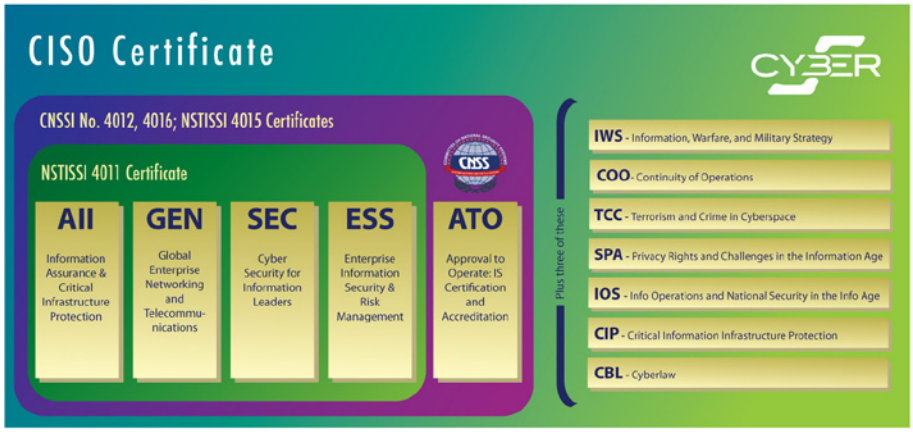
On Thursday, June 14, 2011, the Honorable William J. Lynn, Deputy Secretary of Defense, gave a speech at the National Defense University in Washington, DC, on "Defense Cybersecurity Forum: A New Strategy for Defense." Gen James Cartwright, Vice Chairman of the Joint Chiefs of Staff, joined Lynn to answer questions from the press.

Cyber Security (Cyber-S) Program

Administrating Department: Cyber Integration and Information Operations Department
Department Chair: Mr. Gilliam R. Duvall

The Cyber-S program is a source of graduate-level information security education for those serving as the Chief Information Security Officer (CISO), Senior Agency Information Security Officers (SAISO), their staffs, and cyber security managers. This program provides advanced education to respond to the requirements set forth in the Federal Information Security Management Act (FISMA) and requirements for secure use of national security information systems set by the Committee for National Security Systems (CNSS).

The Cyber Security (Cyber-S) program prepares graduates to:



- Exercise strategic leadership and critical thinking in the development and use of cyber security strategies, plans, policies, enabling technologies, and procedures in cyberspace
- Develop and lead programs to provide cyber security, security awareness training, risk analysis, certification and accreditation, security incident management, continuity of operations, and disaster recovery
- Link people, processes, information, and technology to critical cyber mission decisions to share information in a secure environment
- Develop and lead, in accordance with laws and regulations, an enterprise IA program that promotes and attains national security, agency, and inter-agency goals.

Cyber-S Certificates - 4011; 4012/15/16; CISO

	Course	Course Title
NSTISSI 4011 Certificate (4 Courses Required)		
	AII	Information Assurance and Critical Information Infrastructure Protection
	ESS	Enterprise Information Security and Risk Management
	SEC	Cyber Security for Information Leaders
	GEN	Global Enterprise Networking and Telecommunications
CNSSI No. 4012, 4016, NSTISSI 4015 Certificates (5 Courses Required)		
4011 + ATO	ATO	Approval to Operate
CISO Certificate (8 Courses Required)		
4012 + 3 courses	COO	Continuity of Operations (Required)
	CBL	Cyberlaw (Required)
	IOS	Information Operations and National Security in the Information Age
	IWS	Information, Warfare, and Military Strategy
	SPA	Privacy Rights and Civil Liberties
	CIP	Critical Information Infrastructure Protection
	TCC	Terrorism and Crime in Cyberspace

Government Information Leadership (GIL) MS Degree
Cyber Security (Cyber-S) Concentration
13 Courses Required

	Course	Course Title
Foundational (3)		
	GLS	Global Strategic Landscape
	OCL	Organizational Culture for Strategic Leaders
	CAP	Capstone Course
Leadership (2)		
	AII	Information Assurance and Critical Information Infrastructure Protection (Required)
	DMG	Decision Making for Government Leaders
	IPL	Information Technology Program Leadership
	MAC	Multi-Agency Information-Enabled Collaboration
	LDC -or - SLP	Leadership in the Information Age Strategic Leader Theory and Practice (AMP Students Only)
Management (2)		
	COO	Continuity of Operations
	GIC	Governance in Cyberspace
	IPC	International Perspectives on Cyberspace
	ITP	Information Technology Project Management
	TCC	Terrorism and Crime in Cyberspace
Technology (1)		
	GEN	Global Enterprise Networking and Telecommunications
Core (5)		
	ESS	Enterprise Information Security and Risk Management (Required)
	SEC	Cyber Security for Information Leaders (Required)
	ATO	Approval to Operate
	CBL	Cyberlaw
	CIP	Critical Information Infrastructure Protection
	IOS	Information Operations and National Security in the Information Age
	IWS	Information, Warfare, and Military Strategy
	SPA	Privacy Rights and Civil Liberties

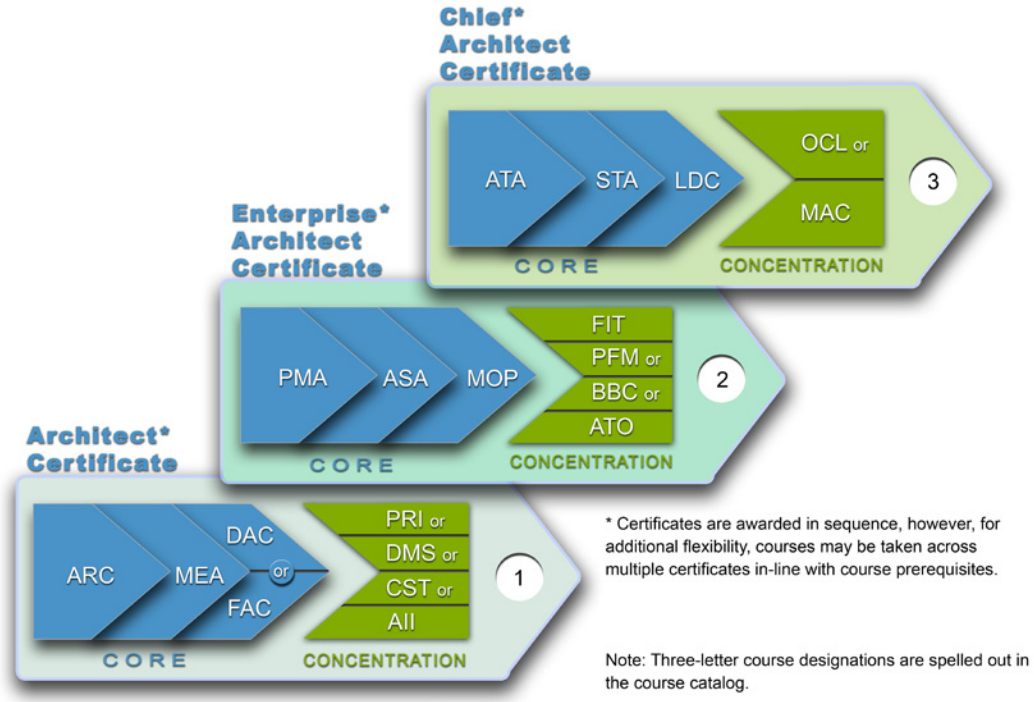
Enterprise Architecture (EA) Program

Administrating Department: Systems and Technology Department
Department Chair: Mr. Andrew P. Gravatt

The Enterprise Architecture (EA) Program prepares architects with the leadership, policy, and technical competencies required for the three levels of EA responsibilities recently identified by the Office of Personnel Management. The NDU iCollege's EA programs consist of three certificates (Architect, Enterprise Architect, and Chief Architect) that document increasing levels of technical and leadership competence. Generally, courses may be completed in any order; however, a few courses have prerequisites. Before being awarded the next level certificate, the student must successfully complete the four courses for it and all courses required for any prior level certificates. As each certificate is completed, graduates grow in their knowledge and ability to lead the application of Department of Defense and other federal approaches, methods, techniques, and work products. Students enrolled in and graduated from the former EA Certificate Program who wish to earn the new certificates will be advised on a case-by-case basis. EA is also a concentration in the Government Information Leader Master of Science degree program

Government leaders who successfully complete the program are empowered to:

- Lead the development, implementation, and management of an EA to support organizational effectiveness, efficiency, and strategic planning
- Leverage people, capabilities, and technology to shape an organization's current and target environments and implement a plan to transition to a successful future
- Meet their Clinger-Cohen responsibilities for "developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the executive agency"



EA Certificates
4 Courses for Each Level

Key Competency	Course	Course Title
Architect Certificate (4 Courses)		
Core (3)	ARC	Enterprise Architecture for Leaders
	MEA	Modelling for Enterprise Architects
	DAC -or- FAC	Defense Enterprise Architecture Federal Enterprise Architecture and Advanced Concepts
Elective (1)	AII	Information Assurance and Critical Information Infrastructure Protection
	CST	Critical Information Systems Technologies
	DMS	Data Management Strategies and Technologies
	PRI	Strategies for Process Improvement
Enterprise Architect Certificate (4 Courses + Architect Certificate)		
Core (3)	PMA	Planning and Managing EA Programs
	ASA	Analytics and Simulation for Enterprise Architecture
	MOP	Measuring Results Organizational Performance
Elective (1)	FIT	Technology Forecasting and Agency Adoption
	ATO	Approval to Operate
	BBC	Building an IT Business Case
	PFM	Capital Planning and Portfolio Management
Chief Architect Certificate (4 Courses + Enterprise Architect Certificate)		
Core (3)	ATA	Advanced Strategies for Enterprise Architecture
	STA	Solutions Architecture and Transition Planning for Architects
	LDC -or- SLP	Leadership in the Information Age -or- Strategic Leader Theory and Practice (AMP Students Only)
Elective (1)	MAC	Multi-Agency Information-Enabled Collaboration
	OCL	Organizational Culture for Strategic Leaders

Government Information Leadership (GIL) MS Degree
Enterprise Architecture (EA) Concentration
13 Courses Required

	Course	Course Title
Foundational (3)		
	GLS	Global Strategic Landscape
	OCL	Organizational Culture for Strategic Leaders
	CAP	Capstone Course
Leadership (2)		
	ARC	Enterprise Architecture for Leaders (Required)
	AII	Information Assurance and Critical Information Infrastructure Protection
	DMG	Decision Making for Government Leaders
	SCL	Strategic Communications for Government Leaders
	IPL	Information Technology Program Leadership
	MAC	Multi-Agency Information-Enabled Collaboration
	LDC -or- SLP	Leadership in the Information Age Strategic Leader Theory and Practice (AMP Students Only)
Management (2)		
	MOP	Measuring Results Organizational Performance (Required)
	BCP	Budget and Congressional Relations for Strategic Leaders
	COO	Continuity of Operations
	ITP	Information Technology Project Management
	PRI	Strategies for Process Improvement
Technology (1)		
	CST	Critical Information Systems Technologies
	DMS	Data Management Strategies
Core (5)		
	FIT -or- ATO -or- BBC -or- PFM	Technology Forecasting and Agency Adoption Approval to Operate Building an IT Business Case Capital Planning and Portfolio Management
	ASA	Analytics and Simulation for Enterprise Architecture (Required)
	MEA	Modelling for Enterprise Architects (Required)
	PMA	Planning and Managing EA Programs (Required)
	DAC -or- FAC	Defense Enterprise Architecture Federal Enterprise Architecture and Advanced Concepts

Government Strategic Leader (GSL) Program

Administrating Department: Information Strategies Department
Department Chair: Dr. John T. Christian

Today the most seasoned government leaders face extraordinary challenges in managing resources, information technologies, social networks, and leading globalized responses. As strategic leaders, they must respond to rapidly evolving national priorities and a dynamic environment. The NDU iCollege's GSL Program provides government leaders the essential tools and strategies required to lead dynamic, complex, and diverse 21st Century organizations. The curriculum engages participants in understanding their organization's unique role and those of other organizations, and how to collaborate to achieve organizational, inter-agency, and national mission and goals. Participants form a learning community to share knowledge, analyze and leverage strategic resources (human, technological, and financial), and create and articulate a vision for themselves and their organizations.

To earn the Government Strategic Leader Certificate, students must complete eight (8) graduate-level courses that may be taken in any order. Two (2) foundation courses are required that focus on organizational culture and the dynamic landscape of government and security. Students select two (2) additional courses in management, two (2) in leadership, and two (2) in technology to meet their professional and/or organizational needs. GSL is also offered as a concentration in the Government Information Leadership Master of Science degree program.

Dr. John Christian, Chair, Information Strategies Department

GSL Certificate
8 Courses Required

Key Competency	Course	Course Title
Core (2)		
	GLS	Global Strategic Landscape
	OCL	Organizational Culture for Strategic Leaders
Management (2)		
	COO	Continuity of Operations
	ESP	Enterprise Strategic Planning
	ESS	Enterprise Information Security and Risk Management
	GIC	Governance in Cyberspace
	ITA	Strategic Information Technology Acquisition
	ITP	Information Technology Project Management
	MOP	Measuring Results Organizational Performance
	PFM	Capital Planning and Portfolio Management
	PRI	Strategies for Process Improvement
	TCC	Terrorism and Crime in Cyberspace
Leadership (2)		
	ARC	Enterprise Architecture for Leaders
	DMG	Decision Making for Government Leaders
	IPL	Information Technology Program Leadership
	LCW	Leading the 21st Century Workforce
	LDC -or- SLP	Leadership in the Information Age Strategic Leader Theory and Practice (AMP Students Only)
	MAC	Multi-Agency Information-Enabled Collaboration
	SCL	Strategic Communication for Government Leaders
Technology (2)		
	CIP	Critical Information Infrastructure Protection
	CST	Critical Information Systems Technologies
	DMS	Data Management Strategies and Technologies
	EIT	Emerging Information Technologies
	GEN	Global Enterprise Networking and Telecommunications
	SEC	Cyber Security for Information Leaders
	WGV	Web-Enabled Government

Government Information Leadership (GIL) MS Degree
Government Strategic Leader (GSL) Concentration
13 Courses Required

	Course	Course Title
Foundational (3)		
	GLS	Global Strategic Landscape
	OCL	Organizational Culture for Strategic Leaders
	CAP	Capstone Course
Leadership (4)		
	ARC	Enterprise Architecture for Leaders (Required)
	DMG	Decision Making for Government Leaders
	IPL	Information Technology Program Leadership
	LCW	Leading the 21st Century Workforce
	LDC -or- SLP	Leadership in the Information Age Strategic Leader Theory and Practice (AMP Students Only)
	MAC	Multi-Agency Information-Enabled Collaboration
	SCL	Strategic Communications for Government Leaders
Management (2)		
	COO	Continuity of Operations
	ESP	Enterprise Strategic Planning
	ESS	Enterprise Information Security and Risk Management
	ITA	Strategic Information Technology Acquisition
	ITP	Information Technology Project Management
	MOP	Measuring Results Organizational Performance
	PFM	Capital Planning and Portfolio Management
	PRI	Strategies for Process Improvement
	TCC	Terrorism and Crime in Cyberspace
Technology (2)		
	CIP	Critical Information Infrastructure Protection
	CST	Critical Information Systems Technologies
	EIT	Emerging Technologies
	GEN	Global Enterprise Networking and Telecommunications
	WGV	Web-Enabled Government
Core (2)		
	CIO -or- PRM	CIO 2.0 Roles and Responsibilities Policy Foundations of Information Resources Management (AMP Students Only)
	CTO	CTO Roles and Responsibilities
	GIC	Governance in Cyberspace
	IPC	International Perspective on Cyberspace
	SEC	Cyber Security for Information Leaders
	SPA	Privacy Rights and Civil Liberties
	NIC	National Intelligence and Cyber Policy

Information Operations (IO) Program

Administrating Department: Cyber Integration and Information Operations Department
Department Chair: Mr. Gilliam R. Duvall

The Information Operations (IO) Program prepares future strategic leaders to effectively integrate and employ the information component of national power in the development and execution of national military and security strategy.

Specifically, the IO program prepares students to:

- Shape strategy and policy decisions, acquire and employ new information technologies, and shape interagency relationships and partnerships that protect, defend and assure information infrastructures in support of our national military, economic, and political power and security
- Employ strategic plans and operational concepts that apply the tools and doctrinal principles of information operations, shape theater and strategic campaign plans, and employ IO in support and execution of military plans, capabilities and operations
- Develop US efforts to employ Strategic Communications in support of national security operations and objectives within the "global information battlespace" and apply both information technology and the content it carries in the "worldwide war of ideas".

IO Certificate
8 Courses Required

	Course	Course Title
Core (8)		
	AII -or-SIO	Information Assurance and Critical Information Infrastructure Protection -or-Protection of Strategic Infrastructure Operations
	CIP	Critical Information Infrastructure Protection
	CST	Critical Information Systems Technologies
	IOS	National Security in the Information Age
	IWS	Information, Warfare, and Military Strategy
	SCL	Strategic Communication for Government Leaders
	SEC	Cyber Security for Information Leadership
	JIOPC	Joint Information Operations Planning Course

Dr. John Saunders, Cyber Integration and Information Operations Department

Government Information Leadership (GIL) MS Degree
Information Operations (IO) Concentration
13 Courses Required

	Course	Course Title
Foundational (3)		
	GLS	Global Strategic Landscape
	OCL	Organizational Culture for Strategic Leaders
	CAP	Capstone Course
Leadership (2)		
	SCL	Strategic Communications for Government Leaders (Required)
	DMG	Decision Making for Government Leaders
	IPL	Information Technology Program Leadership
	LCW	Leading the 21st Century Workforce
	LDC -or- SLP	Leadership in the Information Age Strategic Leader Theory and Practice (AMP Students Only)
	MAC	Multi-Agency Information-Enabled Collaboration
Management (2)		
	COO	Continuity of Operations (Required)
	ESP	Enterprise Strategic Planning
	ESS	Enterprise Information Security and Risk Management
	GIC	Governance in Cyberspace
	ITP	Information Technology Project Management
	MOP	Measuring Results Organizational Performance (Required)
	PRI	Strategies for Process Improvement
	TCC	Terrorism and Crime in Cyberspace
Technology (1)		
	SEC	Cyber Security for Information Leaders
Core (5)		
	AII -or- SIO	Information Assurance and Critical Information Infrastructure Protection -or- Protection of Strategic Infrastructure Operations
	CIP	Critical Information Infrastructure Protection
	IOS	National Security in the Information Age
	IWS	Information, Warfare, and Military Strategy
	JIOPC	Joint Information Operations Planning Course

Information Technology Project Management (ITPM) Program and Information Technology Program Management (ITPgM) Program

Administrating Department: Systems and Technology Department
Department Chair: Mr. Andrew P. Gravatt

The Information Technology Program Management (ITPgM) is an umbrella program consisting of two Certificate programs and a concentration in the Government Information Leadership (GIL) M.S. program. The ITPgM program is designed to meet the ever-increasing call for program managers across the federal government. The Information Technology Project Management (ITPM) certificate is designed to assist agencies in complying with Office of Management and Budget (OMB) direction. The OMB requires that project managers qualified in accordance with CIO Council guidance manage all major information technology projects. The ITPM Certificate requires successful completion of a graduate-level curriculum to satisfy competencies established by the Office of Personnel Management (OPM) Interpretive Guidance for Project Management Positions and the CIO Council Clinger-Cohen Core Competencies. The certificate complements general project management training and the ANSI-recognized Guide to the Project Management Body of Knowledge. It also provides formal educational credit, one of the qualifications required for award of the PMI Project Management Professional (PMP) Certificate.

The Information Technology Program Management (ITPgM) certificate and GIL concentration specifically addressed the OPM competencies for the ITPgM career field. Students earn the ITPgM certificate by successfully completing the ITPM certificate and two additional required courses.

ITPM Certificate
6 Courses Required

	Course	Course Title
Core (4)		
	BBC	Building an IT Business Case
	CST	Critical Information Systems Technologies
	ITA	Strategic Information Technology Acquisition
	ITP	Information Technology Project Management
Speciality (2)		
	IPL	Information Technology Program Leadership
	SAL	Software Acquisition Leadership

ITPgM Certificate
8 Courses Required (ITPM + 2 Courses)

Program Management (2)		
	MOP	Measuring Results Organizational Performance
	PFM	Capital Planning and Portfolio Management

Government Information Leadership (GIL) MS Degree
Information Technology Program Management (ITPgM) Concentration
13 Courses Required

	Course	Course Title
Foundational (3)		
	GLS	Global Strategic Landscape
	OCL	Organizational Culture for Strategic Leaders
	CAP	Capstone Course
Leadership (2)		
	IPL	Information Technology Program Leadership (Required)
	ARC	Enterprise Architecture for Leaders
	DMG	Decision Making for Government Leaders
	LDC -or- SLP	Leadership in the Information Age Strategic Leader Theory and Practice (AMP Students Only)
	MAC	Multi-Agency Information-Enabled Collaboration
	SCL	Strategic Communications for Government Leaders
Management (2)		
	ITA	Strategic Information Technology Acquisition
	PFM	Capital Planning and Portfolio Management
Technology (1)		
	DMS	Data Management Strategies and Technologies
	EIT	Emerging Technologies
	GEN	Global Enterprise Networking and Telecommunications
	SEC	Cyber Security for Information Leaders
	WGV	Web-Enabled Government
Core (5)		
	BBC	Building an IT Business Case
	CST	Critical Information Systems Technologies
	ITP	Information Technology Project Management
	MOP	Measuring Results Organizational Performance
	SAL	Software Acquisition Leadership

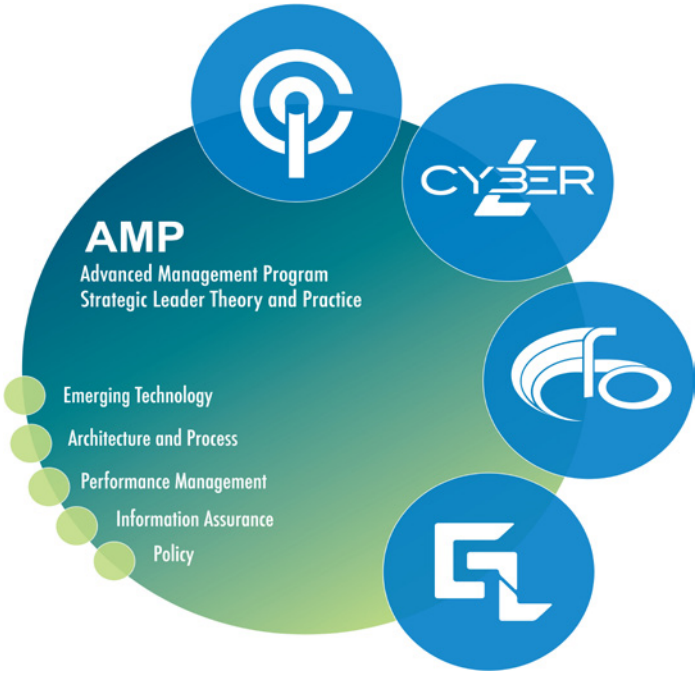
Advanced Management Program

The Advanced Management Program (AMP) is a 14-week intensive resident graduate program designed for middle-and senior-level managers and leaders responsible for promoting and attaining national and international security goals through the strategic use of information and information technology. The AMP is a highly interactive student-centered educational experience in which leadership skills and abilities are emphasized. AMP students form a learning community that fosters multiple perspectives on a wide range of issues. They share knowledge and best practices, strive to become better leaders and decision makers, and master the tools of lifelong learning. Interaction with fellow students, faculty, and government executive guest speakers provides a network of peers throughout the United States public and private sectors and internationally.
The graduate-level AMP curriculum core and elective courses provide participants with the option of earning a Chief Information Officer (CIO) Certificate, Cyber Leadership (Cyber-L) Certificate, Chief Financial Officer (CFO) Leadership Certificate, or Government Strategic Leader (GSL) Certificate. Information Assurance Scholarship Program students must select the CIO Certificate concentration and complete three of the four courses for the Information Assurance 4011 Certificate. The fourth course must be completed before attending AMP.

AMP applicants are eligible for dual admission to the Master of Science in Government Information Leadership. See the Admission Policies section for information

Chief Information Officer Certificate

The CIO Certificate, sponsored by the DOD CIO and the Federal CIO Council is the recognized graduate education for Federal CIO leaders. The CIO Certificate is designed to develop CIO leaders and agency personnel who can leverage the information component of national power for strategic advantage. Refer to the section on the CIO Certificate for complete information.



Cyber Leadership Certificate

The Cyber Leadership (Cyber-L) certificate connects secure information sharing and collaboration across U.S. government agencies, the international community, and the private sector. This program develops leadership skills critical to successfully navigate the current cyberspace domain and promote future integration of cyberspace with the physical domain. Refer to the section on the Cyber-L Certificate for complete information.

Chief Financial Officer Leadership Certificate

The CFO Leadership Certificate is designed to develop the next generation of leaders in government financial management. This certificate leverages the NDU iCollege's current leadership courses while concentrating on the challenges and opportunities facing members of the government financial community, including personnel who work in accounting and finance, budget and cost analysis, auditing, and resource management. Refer to the section on the CFO Leadership Certificate for complete information.

Government Strategic Leader Certificate

The GSL Certificate provides government managers and leaders with the essential tools and strategies required to lead dynamic, complex, and diverse 21st Century government organizations. The curriculum engages participants in understanding their organization's unique role and those of other organizations, and how to collaborate to achieve organizational, inter-agency, and national mission and goals. Refer to the section on the GSL Certificate for complete information.

Approximately two weeks before students' arrival for the 14-week resident AMP, the Office of Student Services emails an elective selection form to each student, asking them to select from available electives such that the certificate requirements in their area of concentration will be satisfied. Queries are addressed by the AMP Director. Refer to the Student Services Section for fees and payment instructions.

AMP Offerings

AMP 44: January 23, 2012 – April 27, 2012;
Applications due November 1, 2011;
Early applications due October 15, 2011

AMP 45: September 10, 2012 - December 14, 2012
Applications due July 1, 2012
Early applications due June 15, 2012

AMP Application Instructions

(Refer to the Student Services and Policies section for AMP and Master of Science Dual Admission information)

Eligibility Requirements

Federal civil service pay grade of GS/GM-12 or equivalent/military officer rank of O-4 or above. Non-federal employees, to include state and local government, must be of an equivalent grade. Private sector employees must be of an equivalent grade and work in a field relevant to the iCollege curriculum and sponsored by a government agency. Private sector employees must provide a resumé detailing last 5 years of employment history as part of their application.

Education: All students must possess a bachelor's degree from a regionally accredited U.S. institution or the equivalent from a foreign institution.

Application Instructions

Federal Government: Applications should be submitted through agency channels and received at the NDU iCollege prior to the published deadline. Each application must contain a résumé, a letter of nomination from the supervisor, and a completed AMP application form (http://www.ndu.edu/icollege/AMP Application Form.pdf). Omission of required information may result in rejection of the application. Incomplete applications will be held by the NDU iCollege for 60 days and then destroyed.

Résumé

The résumé should include a work history that describes the candidate's position titles, organizations, responsibilities, and accomplishments, and any rewards or recognitions received. If there are gaps in the résumé, a short paragraph is needed to explain them.

Nomination Letter

The letter of nomination should address the applicant's ability to complete a challenging graduate-level academic program in information resources management. In addition, the letter must indicate why the applicant is being nominated for the AMP and how this program will benefit the nominating organization. Letters must be on organizational or corporate letterhead and be addressed to the NDU iCollege Office of Student Services. The subject line must indicate the student's name and the program the student is applying for. For example: "Subj: AMP Letter of Nomination, LTC John Doe." The final signature on all correspondence must belong to the applicant's immediate supervisor.

State and Local Government and Private Industry

Applications for AMP must include a résumé, a letter of nomination from a direct supervisor, and a completed copy of the AMP application form.

Submit applications to the NDU iCollege Office of Student Services via fax (202-685-4860), e-mail to iCollegeOSS@ndu.edu or postal mail to:

NDU iCollege
Office of Student Services
300 5th Ave., Bldg. 62
Fort McNair, D.C. 20319-5066

International Students

Non-U.S. citizens who are members of defense agencies of other countries must apply through their governments. Applications should be in the form of an education and training request for approval and processing through the appropriate Security Assistance Training Field Activity (SATFA) country program manager, who should forward the request to:

Fort Monroe, VA 23651-1003
DSN: 680-3255
Commercial: (757) 788-3255
Fax: (757) 788-4142
http://www.satfa.monroe.army.mil/

International students must demonstrate comprehension

Elizabeth McGrath, Deputy Chief Management Officer of the Department of Defense, speaks at the 42nd Advanced Management Program Class Convocation

through listening, reading, and general grammar structures via the Defense Language Institute's English Comprehension Level (ECL) Exam with a score of at least 85 prior to acceptance. Students will take the exam in their home country. Because of the seminar-based active-learning model used in this program, oral communication skills are critical. The NDU iCollege reserves the right to administer the ELC exam after the student arrives per AR 12-15, the Joint Security Assistance Training (JSAT) regulation, Section 10, if English comprehension is in question. International students should also possess basic competencies in the use of personal computers.

Questions about AMP admissions or requirements should be addressed to the Office of Student Services via phone (202-685-6300), or e-mail to iCollegeOSS@ndu.edu.

"We value our partnership with the iCollege of the US National Defence University to deliver high-quality capability development programs to Singapore and regional audiences. We are extremely impressed by the achievements, scholarship and professionalism of the iCollege faculty. Dr Childs and his team are a delight to work with."

Swee Cheang Lim
Director/CEO, Institute of Systems Science
National University of Singapore

Course Descriptions

AII

Information Assurance and Critical Infrastructure Protection (6203)

This course provides a comprehensive overview of information assurance and critical information infrastructure protection. Information assurance of information assets and protection of the information component of critical national infrastructures essential to national security are explored. The focus is at the public policy and strategic management level, providing a foundation for analyzing the information security component of information systems and critical infrastructures. Laws, national strategies and public policies, and strengths and weaknesses of various approaches are examined for assuring the confidentiality, integrity, and availability of critical information assets.

Learning Outcomes: Students will be able to analyze laws, national strategies, and public policies; and assess the strengths and weaknesses of various approaches for assuring the confidentiality, integrity, and availability of those information created, stored, processed, and communicated by information systems and critical information infrastructures.

ARC

Enterprise Architecture for Leaders (6412)

This course examines enterprise architecture (EA) as a strategic capability organizational leaders use for enterprise planning, resource investment, management decision-making, and key process execution. Students explore leadership competencies and strategies needed to advance EA adoption and assess the integration of EA with governance, strategic planning, budgeting, portfolio management, capital planning, and information assurance. They critique EA prescriptive frameworks that guide EA development activities and review EA evaluative frameworks used to assess organizational EA management capacity and capability. Students evaluate challenges to organizational EA adoption and consider strategies to address them.

Learning Outcomes: Students will be able to evaluate the nexus between enterprise architecture (EA) and successful enterprise planning and operations, EA's role in facilitating other critical agency activities, e.g., budgeting, capital planning, and investment control (CPIC) and information assurance (IA), the application of EA models, and strategies to address the challenges of EA adoption, use, and institutionalization

ASA

Analytics and Simulation for Enterprise Architecture (6436)

Prerequisites: MEA

This course examines analytical techniques and simulation models through analysis and evaluation of qualitative and quantitative data sets. Students use descriptive analytics and statistics to collect, categorize and analyze data to discover numerical and visual patterns and create usable information. Students explore a sampling of simulation techniques to assess how they can be used to inform enterprise architect practitioners and leaders about new methods of analyzing data in a discreet or continuous manner. Students evaluate different presentation techniques to evaluate their efficacy for highlighting relevant information in the decision-making process.

Learning Outcomes: Students will be able to create and recommend strategies to increase the effectiveness of the EA and EA program's contribution to mission performance through reliable and validated data collection methods, analysis and evaluation of qualitative and quantitative data, and simulation.

ATA

Advanced Strategies in Enterprise Architecture (6437)

Prerequisites: Completion of Level II EA Certificate courses

In this course students examine advanced strategies and topics in enterprise architecture (EA) by building upon and integrating prior academic and professional experiences as EA practitioners. Students appraise alternative EA governance strategies and integration used in industry and public sector. Through an overview approach, students evaluate the OMB EA related policies to determine architectural alignment with an organization's EA. Students evaluate organizational constructs to improve mission performance in the Information Age. Agile organizational characteristics are considered as part of an in-depth exploration of Federated EA concepts.

Learning Outcomes: Students will be able to evaluate and make recommendations based on the effectiveness of the EA and EA program's contribution to mission performance in their organization. Students will create strategies for effectively improving their organization's EA program.

Dr. Mary McCully, Dean of Faculty and Academic Programs (first row-red headscarf), Dr. Russ Mattern, NDU iCollege faculty (first row-blue cap), and AMP 42 students pause "Day in Woods" leadership development activities for a picture.

ATO

Approval to Operate: Information System Certification and Accreditation (6209)

This course examines the information security certification and accreditation principles leading to final Approval to Operate (ATO) an information system. The course examines roles, responsibilities, documentation, organizational structure, directives, and reporting requirements to support the Designated Accrediting Authority (DAA) in approving the security control functionality level of an information system and granting ATO at a specified level of trust. The course provides an overview of DOD and Federal department and agency certification and accreditation processes (e.g., Defense Information Assurance Certification and Accreditation Process; NIST Certification and Accreditation Process), information assurance acquisition management, and system security architecture considerations.

Learning Outcomes: Students will be able to document a certification and accreditation plan, present and justify the plan to senior management for approval, and develop a systems security authorization agreement for their organization.

BBC

Building an IT Business Case (6430)

This course focuses on development and presentation of an effective IT acquisition business case for financial systems and other information technology investment as an essential element of agency IT portfolio management, financial management, and program management. Well-developed business cases support agency IT capital and planning and investment control, agency budget planning, and successful OMB IT investment review. Topics include best practices in economic and risk analysis, identifying and communicating the value of alternative IT investments, business process reengineering and benchmarking, and the IT Program Manager's responsibilities in agency IT portfolio management. The course examines both the OMB Circular A-11 Exhibit 300: Capital Asset Plan and Business Case Summary and the more detailed business case used in the agency investment review and budgeting process. Students analyze sample IT business cases and develop a business case based on source materials.

Learning Outcomes: Students will be able to create a hypothetical IT business case, critique one using a business case evaluation method and other criteria, and recommend changes to improve the process of developing and defending an IT business case.

BCP

Budgeting and Congressional Relations for Strategic Leaders (6605)

This course presents a strategic understanding of Federal budgeting and appropriations, with particular attention to the role of Congress. With this critical understanding, students develop leadership strategies to shape the fiscal environment to achieve agency strategic outcomes. The course focuses on topics such as the impact of current fiscal issues including the competition between discretionary and nondiscretionary spending and its likely impact upon agency activities, the dynamic interaction between agency, executive, and Congressional committees and staffs in developing a budget and gaining an appropriation.

Learning Outcomes: Students will be able to analyze the Federal budgeting and appropriations process, identify contemporary and emerging challenges shaping the federal budget, and evaluate possible impacts upon their agency.

CAP

Capstone (6700)

The CAP course is the culminating learning experience of the Government Information Leadership (GIL) Master of Science Degree Program. While enrolled in CAP, students complete a capstone synthesis project in his or her area of concentration.

Learning Outcomes: Students who have successfully completed the Capstone course will be able to integrate critical concepts from their course work, independent readings, and professional practice; apply this knowledge to the analysis of broad, enduring issues in information leadership in their concentration area; and create and deliver an executive-level project that synthesizes the major themes and conclusions across the concentration in a capstone project.

CBL

Cyberlaw (6204)

This course presents a comprehensive overview of ethical issues, legal resources and recourses, and public policy implications inherent in our evolving online society. Complex and dynamic state of the law as it applies to behavior in cyberspace is introduced, and the pitfalls and dangers of governing in an interconnected world are explored. Ethical, legal, and policy frameworks for information assurance personnel are covered. Various organizations and materials that can provide assistance to operate ethically and legally in cyberspace are examined. Topics include intellectual property protection; electronic contracting and payments; notice to and consent from e-message recipients regarding monitoring, non-repudiation, and computer crime; and the impact of ethical, moral, legal, and policy issues on privacy, fair information practices, equity, content control, and freedom of electronic speech using information systems.

Learning Outcomes: Students will be able to assess potential legal issues that might flow from implementing and not implementing information security policies, practices, and procedures, and create policies and operating procedures for an organization that are ethically and legally sound.

CFF

Changing World of the CFO (6601)

For CFO Program students only

This course focuses on the changing environment for the government Chief Financial Officer (CFO). Students explore the fundamental role of the collaborative and networked community as the critical ingredient of success. The course provides an overview of the essential elements of the current and future roles of government CFO's and their senior staffs. It surveys the various roles of the executive and strategic leader in the world of government financial management including budget officer, compliance officer, internal controls/risk manager, strategic planner, fiduciary reporter, and reporter of management and financial information. The course discusses the policies, challenges and opportunities associated with decision support to management, financial reporting, business process improvement, systems integration, financial systems, workforce development, performance management, budget, and portfolio management. Students discuss standards, accountability, privacy, and transparency issues.

Learning Outcomes: Students will be able to analyze the most pressing governance issues relevant to leading financial transformation in government; evaluate the philosophical perspectives, roles and dynamic relationships of organizations and functional areas impacting the financial communities decision support to leadership; analyze and evaluate the critical integration necessary between financial management functions required to lead an effective CFO organization; and analyze cross government collaboration and the networked community as key facilitators of success for the CFO in the future.

CIO

CIO 2.0 Roles and Responsibilities (6303)

Students examine the essential analytic, relational, technological, and leadership competencies that government CIOs and their staffs need to respond to and shape the 21st Century environment. Students assess the high information and IT demands of customers; examine the potential and perils of ubiquitous technology and information saturation; and weigh the tradeoffs of resource constraints, legal and policy mandates, and security in an open environment. The dynamic and multi-dimensional roles and responsibilities of government CIOs and their staffs are scrutinized to assess opportunities and challenges for improving governance, resource management, and decision making. Students analyze critical internal (CTO, CFO, Commander, Agency Head, Operations Chiefs) and external (other governmental agencies, OMB, Congress, and the private sector) relationships that CIOs and their staffs need to foster in order to satisfy their mission-related, legal, organizational, and political mandates.

Learning Outcomes: Students will be able to analyze the multi-dimensional and shared leadership roles and responsibilities of government CIOs and their staffs; recommend internal and external relationships that CIOs must foster in order to respond to and shape the environment

while meeting their legal, policy, and organizational mandates; and advocate a more active role for CIOs in formulation of policies that have potential impacts from leveraging emerging technologies.

CIP

Critical Information Infrastructure Protection (6230)

This course examines the security of information in computer and communications networks within infrastructure sectors critical to national security. These include the sectors of banking, securities and commodities markets, industrial supply chain, electrical/smart grid, energy production, transportation systems, communications, water supply, and health. Special attention is paid to the risk management of information in critical infrastructure environments through an analysis & synthesis of assets, threats, vulnerabilities, impacts, and countermeasures. Students learn the importance of interconnection reliability and methods for observing, measuring, and testing negative impacts. Critical consideration is paid to the key role of Supervisory Control And Data Acquisition (SCADA) systems in the flow of resources such as electricity, water, and fuel. Students learn how to develop an improved security posture for a segment of the nation's critical information infrastructure.

Learning Outcomes: Students will be able to use a people, process, and technology framework to assess a current strategy and devise an improved security strategy for interconnection or for a specific control systems environment within a national critical infrastructure area.

COO

Continuity of Operations (6504)

This course focuses on developing and implementing effective continuity of operations (COOP) plans in public sector agencies. Using federal regulations and policies as a backdrop, the course examines the technological, human capital, legal, and business factors involved in creating and maintaining a COOP plan. Topics include determining business requirements, selecting alternate sites, employing technology to increase organizational resilience, developing exercises, and creating and implementing emergency plans. Through a series of exercises, students develop skills in creating, evaluating and implementing continuity of operations policies and plans.

Learning Outcomes: Students will be able to analyze current continuity of operations plans for adequacy and compliance with federal law, regulations and best practices, and to develop new continuity of operations plans to address organizational risks and contingencies.

CST

Critical Information Systems Technologies (6510)

This course probes the rapid advances in all aspects of information systems technology from the perspective of both the functional and the information resources manager. The course provides an overview of both the current state of the art and the trends in information systems technology with particular attention to software development technologies, data management, computer systems hardware, human-computer interfaces, voice recognition, natural language understanding, collaborative technologies, telecommunications technologies, and electronic

Professor Andrew Gravatt, Chair, Systems and Technology Department, teaches the first NDU iCollege lesson fully presented in a Virtual World at the NDU iCollege Second Life Campus.

commerce technologies. It concludes with a group exercise designed to determine how a CIO can address the issues these technologies introduce within an organization.

Learning Outcomes: Students will be able to evaluate the usefulness of recent developments in hardware, software, and other information systems to meet organizational goals; develop metrics for measuring the usefulness of the technologies; and determine the best strategy for infusing these technologies into their organizations.

CTO

CTO Roles and Responsibilities(6441)

This course focuses on the multi-faceted role that effective CTOs play in agencies and organizations. Lessons examine how CTOs strategically forecast and assess new technologies, and coordinate the application of technology in an organization to meet current and future organizational needs. Topics include an exploration of how CTOs leverage enterprise architecture as a vehicle to plan for technological change and build strategic partnerships with key stakeholders, industry, and the marketplace to improve business processes and meet strategic goals.

Learning Outcomes: Students will be able to assess the technological maturity and the long-term technology needs of their organization; forecast, assess, and integrate new technologies into an organizational infrastructure using knowledge of acquisition and organizational communication; and develop strategies to adapt emerging technologies to achieve current and future strategic organizational goals while mitigating risks to cyber security.

DAC

Defense Enterprise Architecture (6438)

Prerequisite: ARC

This course presents policies, practices, and strategies to develop and implement enterprise architectures (EA) supporting Department of Defense (DOD) organizations. Students assess in greater detail the DOD Architecture Framework (DODAF) and associated work-products. Students analyze the DOD Defense Information Enterprise Architecture (IEA), Business Enterprise Architecture (BEA), and aspects of the Global Information Grid (GIG).

Learning Outcomes: Students will be able to assess the degree to which an agency's enterprise architecture aligns with the DoD's EA related policy and guidance, and formulate strategies to increase its alignment.

DMG

Decision Making for Government Leaders (6323)

This course examines the environment, opportunities, and challenges of leadership decision making in government agency and interagency settings from individual, managerial, and multi-party perspectives. Decision contexts and the consequences for federal government leaders and organizations are viewed using the multiple perspectives of governance, policy, technology, culture, and economics. Students actively explore and reflect on how and why decisions are made by immersing themselves into complex issue scenarios and using leading-edge decision tools.

Learning Outcomes: Students will be able to analyze leadership decision making and the decision environments in federal government agency and interagency settings; assess the challenges and opportunities for decision makers in federal government collaborative and information-sharing environments; assess decision consequences and outcomes in terms of agency missions, political mandates, and statutory guidance; and determine the types of decision tools appropriate for their organization.

DMS

Data Management Strategies and Technologies: A Managerial Perspective (6414)

This course explores data management and its enabling technologies as key components for improving mission effectiveness through the development of open, enterprise-wide, and state-of-the-art data architectures. It examines management issues such as the implementation of the data component of the Enterprise Architecture specified by OMB. The course considers key data management strategies, including the DOD Net-Centric Data Strategy, and the Federal Enterprise Architecture (FEA) Data Reference Model and their enabling information technologies including data warehousing, electronic archiving, data mining, neural networks, and other knowledge discovery methodologies. Students explore data management issues and implementation. The course provides sufficient insight into the underlying technologies to ensure that students can evaluate the capabilities and limitations of data management options and strategies.

Learning Outcomes: Students will be able to assess an organization's current data architecture and implementation and develop strategies to enhance them to improve agency mission effectiveness.

EIT

Emerging Technologies (6442)

This course examines the core concepts of information technology and its rapidly expanding role in solving problems, influencing decision making and implementing organizational change. Students analyze how emerging technologies evolve. They evaluate the international, political, social, economic and cultural impacts of emerging technologies using qualitative and quantitative evaluation methods. Students assess emerging technologies using forecasting methodologies such as monitoring and expert opinion, examining future trends, and assessing international perspectives.

Learning Outcomes: Students will be able to appraise the impact and utility of emerging technologies; project into the near future the probable progress of emerging trends; formulate policies to guide the adoption of appropriate emerging technology to enhance the workplace and meet organizational mission.

ESP

Enterprise Strategic Planning (6320)

This course reviews and discusses the interagency national security strategic planning process and The National Security Strategy (NSS) of the United States of America. The relationship between the NSS, other supporting national security strategic plans, and agency strategic plans is analyzed. Students are introduced to several approaches to developing strategy in the face of uncertainty, including a new scenario planning approach. Students apply this new scenario planning approach to identify the US national security objectives and robust national capabilities that need to be developed or strengthened, and recommend various means for building these capabilities. Students analyze their organization's role in building these future national security capabilities.

Learning Outcomes: Students will be able to evaluate an organization's strategic plan for robustness against potential futures, identify capability gaps in their organization's strategic plan, and recommend strategies to fill these gaps.

ESS

Enterprise Information Security and Risk Management (6206)

This course explores three themes, based on the Certified Information Security Manager® (CISM®), critical to enterprise information and cyber security management areas: information security risk management, information security/assurance governance, and information security/assurance program management. Examining the concepts and trends in the practice of risk management, the course analyzes their applicability to the protection of information. Information security/assurance governance is illuminated by exploring oversight, legislation, and guidance that influence federal government information security/assurance. The course explores the challenges of implementing risk management and governance through enterprise security/assurance program management. This includes enterprise information and cyber security strategies, policies, standards, controls, measures (security assessment/metrics), incident response, resource allocation, workforce issues, ethics, roles, and organizational structure.

Learning Outcomes: Students will be able to recommend a risk management approach for an enterprise information and cyber security program for their organizations.

Crisis Center, NDU iCollege iLabs

FAC

Federal Enterprise Architecture (6409)

Prerequisite: ARC

This course presents Office of Management and Budget (OMB) guidance for the development and implementation of enterprise architecture for federal, non-Department of Defense (DoD) agencies. Students assess the Federal Enterprise Architecture reference models and profiles and IT investment business cases, the OMB Exhibit 300 and 53. They examine the Federal Segment Architecture Methodology (FSAM), first introduced in Enterprise Architecture for Leaders (ARC). The course concludes with an overview of the DoD Architecture Framework to provide insight into DOD's approach for the development of enterprise architecture.

Learning Outcomes: Students will be able to assess the degree to which an agency's enterprise architecture is consistent with the Federal Enterprise Architecture Segment Methodology and recommend appropriate strategies to improve their agency's enterprise architecture.

FIT

Technology Forecasting and Agency Adoption (6443)

This course explores how federal agencies can adopt mainstream information technology (IT) more effectively in the context of larger movements in the technology industry and within internal agency policy, governance, and processes. Topics are taught from a systems thinking perspective and include the technology adoption process and different methods of technology forecasting. Students develop skills in scanning, monitoring, and investigating the technology industry for innovations that can meet their agency's needs. They explore current and emerging issues in key technologies and encounter different ways of engaging industry to gain deeper understanding of key innovations to help agencies make informed decisions. Students assess their agency's technology adoption process, considering governance, performance measurement, and risk.

Learning Outcomes: Students will be able to develop an implementing strategy to lead successful agency technology adoption through effective policy, governance, and technology forecasting; analyze different methods of technology forecasting, performance and risk management, and industry partnering; and summarize how IT is invented, funded, developed by companies, and then adopted by agencies.

FFR

The Future of Federal Financial Information Sharing (6607)

CFO Certificate students only

This course focuses on the vital role Chief Financial Officers and financial managers have in providing federal financial information. To fully support decision making, this actionable financial information must be timely, accurate, transparent, accountable, and result in "clean" audit opinions. To evaluate the quality of Federal financial information sharing, the course explores the current stovepipes of financial statements, budgetary reporting, program/project cost reporting, and financial standards, as well as a holistic view of crosscutting information such as financial and non-financial dashboards. In addition, successful financial information sharing in the current dynamic environment can be facilitated by financial systems, data management techniques, and effective communication with internal and external users.

Learning Outcomes: Students will be able to identify potential internal and external consumers of Federal financial information and to evaluate the consumers desires and expectations; analyze the changing roles, requirements, and expectations for financial, budget, and program/project financial information in government organizations from legal, policy, and technological perspectives; evaluate financial systems and processes, and data management techniques that support new information sharing challenges; and to design a leadership plan for their organization that responds to current and future expectations for financial information sharing that supports decision making at all levels.

GEN

Global Enterprise Networking and Telecommunications (6205)

This course focuses on the effective management of network and telecommunications technologies in a government-sector global enterprise. The course examines current and emerging network and telecommunications technologies, including their costs, benefits, and security implications, placing emphasis on enabling military and civilian network-centric operations. Topics analyzed include network-centric concepts, spectrum management, data networks and associated Internet technologies, telephony, the role of public policy, and the significance of industry as a service provider and as an engine of innovation.

Learning Outcomes: Students will be able to evaluate the managerial, policy, and security consequences of adopting telecommunications and network technologies and develop a detailed implementation plan to incorporate a technology into an enterprise.

Dr. Cathryn Downes, NDU iCollege Professor shares course innovations with participants at the NDU iCollege 2011 Federal Consortium for Virtual Worlds Conference.

GIC

Governance in Cyberspace (6326)

This course examines several global aspects of cyberspace (according to GAO [2010]), including (1) providing leadership, (2) developing governance strategies, (3) coordinating across relevant entities, (4) ensuring technical standards and policies do not prevent U.S. trade, (5) participating in international cyber incident response, (6) differing legal systems and law enforcement, and (7) defining international norms for cyberspace. By considering various governance models (e.g., geopolitical, non-profit, corporate, and socio-economic) and cyberspace models, the students assesses the merit and impact of governance applied to cyberspace and associated individual and organization rights. The course examines the consequences, the repercussions, and the likely outcomes of implementing diverse cyberspace governance scenarios. Students evaluate and synthesize results toward defining next-generation governance leadership models to address and shape evolving cyberspace domains.

Learning Outcomes: Students will be able to assess models of governance for their applicability to cyberspace; evaluate the impact and outcomes of current governance efforts on individual, organization, and cyberspace performance, and develop strategies of alternate governance models to shape the evolving cyberspace domain.

GLS

Global Strategic Landscape (6213)

This course focuses on two broad themes of the evolving global strategic landscape: how global changes may impact future U.S. national security strategy, and the implications of these developments for creating Information Age government with national security responsibilities. The students examine the major trends that have transformed the world's economic, social, environmental, technological, political, and security landscape during the post-Cold War period, as well as possible future developments in these areas. They explore the implications of these trends for the national security environment, consequent options for national security strategy, and the transformation of Information Age government agencies.

Learning Outcomes: Students will be able to evaluate the impact of economic, social, environmental, political, technological, and international security trends on national security; integrate long-range trends into the development of national security strategy; and develop policy options that take into account these strategic and evolving security trends to transform government agencies into Information Age government organizations.

IOS

Information Operations and National Security in the Information Age (6207)

Prerequisite: Secret Clearance is required

This course examines the essential paradigms and concepts of Information Operations (IO), Information Assurance (IA), and Strategic Communication (SC). It explores the technological revolution and the information component of national power, and examines that component in the National Security Strategy in light of the nature of the interconnected age; existing national policy; organizational transformation; and equities involved in IO, IA, and SC and information as a strategic environment. The course concludes by exploring the new paradigm of national security in the Information Age and the need for an information strategy to support the National Security Strategy.

Learning Outcomes: Students will be able to analyze how the information component of power is used in national security strategies and operations; analyze the role played by IO/IA/SC in national security strategies and operations; synthesize new approaches for the employment of the information component of power in national security strategies and operations; and apply IO/IA/SC in the development and execution of national security strategies and operations.

IPC

International Perspective on Cyberspace (6228)

This course provides an overview of the issues surrounding transnational cyberspace policies, international investment strategies, and implementation of information and communication technologies (ICT) that affect the global economy and transforms the flow of information across cultural and geographic boundaries. Students examine the cyberspace policies that empower ICT innovation, various global governance frameworks, and organizations that shape and transform cyberspace, to include the Internet Corporation for Assigned Names and Numbers (ICANN), the International Telecommunications Union (ITU), the World Bank Information and Communications Technology Sector, and the U.S. Federal Communications Commission (FCC).

Learning Outcomes: Students will be able to formulate and implement international strategies to promote an open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and innovation. They will be able to assess and recommend critical success factors which build and sustain an environment in which cyber norms of responsible behavior guide nation states' actions, sustain public and private sector partnerships, and support transnational rules of law in cyberspace.

IPL

Information Technology Program Leadership (6411)

This course examines the challenges of Federal program leadership in an Information Technology (IT) context. Students gain theoretical insight, supplemented by practical exercises, covering a variety of program/project leadership concepts and techniques. Particular areas of focus include customer service, stakeholder relations, decision-making methods, processes and pitfalls, interpersonal skills, organizational awareness and dynamics, and written and oral communication skills. The course explores the role of oversight in the management and leadership of Federal IT acquisition programs.

Learning Outcomes: Students will be able to evaluate leadership challenges likely to arise in managing an IT project, identify and implement appropriate strategies to manage them successfully, and communicate project plans and technical content effectively, either orally or in writing.

ITA

Strategic Information Technology Acquisition (6415)

This course examines the role senior leaders in both government and industry play in the successful acquisition of information technologies and services to achieve strategic organizational goals. Using the framework of the systems development life-cycle, it explores regulatory policies, acquisition strategies, requirements management, performance measurement, and deployment and sustainment activities that directly impact IT acquisition. Acquisition best practices such as performance-based contracting, risk management, use of service-level agreements, trade-off analyses, as well as the pros and cons for use of commercial off-the-shelf products are explored. Significant focus is placed on contracting issues including; the role of the contracting officer, building a solid request-for -proposal, how to prepare for and run a source selection and the role of oral presentations.

Learning Outcomes: Students will be able to evaluate agency information technology acquisition programs using a systems development life-cycle framework to identify and correct deficiencies in strategy, requirements, design, development, test, deployment and sustainment.

ITP

Information Technology Project Management (6416)

This course focuses on project and program management in an Information Technology (IT) context, including financial systems. Students explore industry-accepted project management processes, e.g., the Project Management Institute's (PMI) Project Management Body of Knowledge (PMBOK) framework, and apply project management concepts. Major topics include planning and management of project communications, scope, time, cost, quality, risk, human resources, procurement, and project integration. Factors that make IT projects unique and difficult to manage are explored, along with tools and techniques for managing them. This course challenges students to gain hands-on project management experience by performing complex project management tasks leading to the development of a project management strategy/plan.

Learning Outcomes: Students will be able to assess a project management strategy/plan and develop a plan for an IT project.

IWS

Information, Warfare, and Military Strategy (6202)

Prerequisite: Secret Clearance is required.

This course examines key considerations for the planning and conduct of information operations at the theater and strategic levels. The course emphasizes inter-agency and international considerations in the planning and conduct of Information Operations (IO). Students examine selected non-U.S. approaches to the strategies for and uses of the full spectrum of information operations by current and potential global competitors and adversaries. They examine strategic legal implications and considerations and the use/misuse of IO strategies against an adaptive adversary. The course concludes with a snapshot of current U.S. military IO strategies.

Learning Outcomes: Students will be able to evaluate the specific capabilities and potential contributions of the designated IO organizations, capabilities, and planning tools; evaluate and integrate IO requirements and capabilities within the appropriate phases of the deliberate and crisis planning processes; ascertain the contributions and limitations of IO within a strategic/theater strategic context; compare and contrast selected non-U.S. approaches to and uses of IO; and design an appropriate military strategy for the employment of IO capabilities over a time horizon suited to the effects to be achieved.

LCW

Leading the 21st Century Workforce (6506)

The LCW course provides leaders and managers with knowledge and tools that enhance their capacity to lead the 21st Century workforce effectively in the achievement of organizational objectives. Using a blend of leadership theory and best practice research, the course explores the dynamics of an increasingly diverse workforce, complex environment, ubiquitous technology, information saturation, and evolving work and organizational contexts. Students take an in-depth view of their self leadership, interpersonal leadership, and organizational leadership in order to develop themselves as leaders. They explore strategies to achieve their organization's goals through self-awareness, learning agility, coaching and mentoring, talent management, teaming, and cross-boundary influence, and to foster and manage innovation, leverage generational diversity, create a collaborative culture, facilitate knowledge management, and engender high-trust ethical practices.

Learning Outcomes: Students will be able to analyze emergent and proven perspectives of leadership and influence, and create effective strategies to develop, shape and lead a thriving 21st Century government workforce

Dr. Mike Piller, NDU iCollege Director of Academic Computing and Laboratories delivering a presentation with a touch screen monitor.

Dr. Mark McGibbon, Lockheed Martin Visiting Faculty to the NDU iCollege

LDC

Leadership for the Information Age (6301)

This course examines Information Age leadership and organizations. It describes the successful Information Age leader and organization as constantly learning and adapting to an increasingly complex, changing, and information-rich environment. Emphasis is placed on "out-of-the-box" thinking, individual and organizational innovation, and the processes and structures that enhance an organization's ability to learn, adapt, and compete in the Information Age. The course explores the role of information and technology in the Information Age organization; the relationships among learning, change, and strategic planning; and the new abilities required for leading in the Information Age.

Learning Outcomes: Students will be able to demonstrate effective collaboration and teamwork across various problem-solving circumstances, and create and design effective processes and structures that increase organizational flexibility and agility.

MAC

Multi-Agency Information-Enabled Collaboration (6512)

The course focuses on multi-agency collaboration in support of national and homeland security and national preparedness planning, decision-making and implementation. It examines current and proposed strategies, means and models for substantially improving the effectiveness of collaboration at the federal, state and local levels, and beyond to include multilateral situations with non-governmental, media, and international organizations and coalition partners. The course assists students to synthesize the underlying principles that define effective collaboration, and critical lessons learned from past challenges and current experiments. Legal, budgetary, structural, cultural and other impediments that inhibit inter-agency mission effectiveness are assessed, as are strategies for addressing them. The course explores evolving network structures, collaborative tool-sets including social media, cross-boundary information-sharing and work processes, emergent governance arrangements, and the behaviors and skills of collaborative leadership as a key component of government strategic leadership

Learning Outcomes: Students will be able to formulate and shape strategic, operational or tactical-level initiatives aimed at improving effectiveness in missions that critically depend upon multi-agency collaboration; appraise critically the ends, ways, and means including tools, technologies, and work practices, of highly effective multi-agency collaborations; and develop, propose, and defend recommendations for initiatives aimed at effective multi-agency collaboration and their supporting execution and transition plans.

MEA

Modeling for Enterprise Architecture (6439)

Prerequisite: ARC or instructor permission. Students must be able to install a provided EA modeling repository tool on a non-iCollege computer.

This course explores the use and effectiveness of architectural modeling to describe an organization and examines model-based products to support, influence, and enable organization planning, and decision-making. Students

gain practical experience with work-products common to the DOD Architecture Framework (DODAF) and OMB Federal Segment Architecture Methodology (FSAM), as well as other established frameworks. Models examined in the course include: object-oriented models (e.g., Unified Modeling Language (UML)) covering process, data, and systems; and Structured models (e.g. IDEF). Emphasis is placed on the efficacy of modeling styles and the interpretation of the descriptive models.

Learning Outcomes: Students will be able to accurately interpret object-oriented and structured-based diagrams and evaluate the primary characteristics of a model to validate its quality.

MOP

Measuring Results of Organizational Performance (6316)

This course is an executive view of strategic planning and performance management in public organizations. Using the Balanced Scorecard as a framework, students examine the linkage of mission to strategic planning, performance management, performance measurement, operational strategies, initiatives, and budgets to support decision making. Emphasis is on transparency and organizational outcomes. Students determine and apply appropriate data tools, collection techniques, analysis, and reporting when assessing their organization's performance.

Learning Outcomes: Students will be able to integrate strategic planning and performance management principles into a public-sector organization assessment to support senior decision-making and strategic communications. They will be able to develop and/or assess a comprehensive plan for conducting a performance assessment in their organization that directly supports senior decision makers in achieving mission effectiveness.

NIC

National Intelligence & Cyber Policy (6229)

This course provides an overview of intelligence information and cyber policy as elements of national power to include planning, collection, processing, analysis, dissemination and exploitation. It describes the organizations that comprise the intelligence community and their relationships, how the intelligence budget works, and the congressional oversight that provides checks and balances on the management of the intelligence community by the executive branch. It also examines the cyber policies and standard operating procedures for organizations that support national intelligence, counterintelligence, and cybersecurity program functions.

Learning Outcomes: Students will be able to discuss intelligence and use of cyberspace policy as elements of national power and describe the intelligence community and how it informs statecraft.

OCL

Organizational Culture for Strategic Leaders (6321)

This course explores the strategic and persistent effects of culture on mission performance. Students examine the ways in which leaders can employ this powerful influence to nurture organizational excellence or to stimulate changes in organizational behavior. They investigate organizational sciences for traditional and Information Age perspectives on organizational behavior, on frameworks for assessing organizational cultures, and on strategies to initiate and institutionalize strategic mission-oriented change. Cross-boundary, inter-agency, cross-generational, and global influences, issues, and challenges are examined from a cultural perspective.

Learning Outcomes: Students will be able to assess the culture of an organization within its strategic context, understand culture's critical role in processes and decision making, and design strategic initiatives to either sustain or change the organizational culture to support organizational missions that effectively contribute to Information Age government.

PFM

Capital Planning and Portfolio Management (6315)

This course focuses on state-of-the-art strategies for portfolio management, with an emphasis on assessing, planning, and managing information technology (IT) as a portfolio of projects from the perspectives of CIOs and CFOs. The three phases of the investment management process are considered: selection, control, and evaluation of proposals; on-going projects; and existing systems. The relationship of performance measures to mission performance measures is explored. The course examines the roles of the CIO, the CFO, and other managers in developing investment assessment criteria, considers how the criteria are used in planning and managing the portfolio, and explores the Office of Management and Budget's (OMB) portfolio perspective as found in Circular A-11, Part 7, Section 53, Information Technology and E-Government. Individual and team exercises are employed, including simulation of an IT investment portfolio review by the Investment Review Board.

Learning Outcomes: Students will be able to evaluate an investment portfolio and the corresponding capital planning and investment management process to ensure that they comply with current statutes and regulations, recommend changes to the process, and develop a strategy for balancing a portfolio of investment projects.

PMA

Planning and Managing Enterprise Architecture Programs (6432)

Prerequisite: DAC or FAC

Students examine the management of enterprise architecture (EA) as a continuous organizational program. They analyze critical EA program management success factors such as obtaining and maintaining organizational leadership commitment, building effective EA program management teams, and selecting an appropriate EA methodology. Students develop actionable EA program plans for: management, governance, and strategic communication; and develop requirements for select EA-support tool(s).

Learning Outcomes: Students will be able to develop effective programs plans for an enterprise architecture program that responds to organizational priorities, culture and constraints.

PRI

Strategies for Process Improvement (6333)

This course examines strategies, management processes and resources for process improvement within and across Federal agencies. The course provides an executive-level examination of business process improvement strategies, including business process re-engineering, activity-based costing/management, process architecting, Lean Six Sigma, and other quality improvement programs. An overview of the techniques and technologies that enable process-centric performance improvements in how agencies achieve their missions is provided. Attention is focused on the enterprise-level leadership challenges of process management, including initiation, collaboration, design, implementation, and portfolio project management of process-centric improvements within and across agencies.

Learning Outcomes: Students will be able to recommend appropriate process change strategies, tools, and methods for carrying out process improvement. They will be able to provide advice on the implementation challenges of process improvement, including impacts upon organizational culture, structure and governance, and design, and propose initiatives and actions for addressing such challenges.

PRM

Policy Foundations of Information Resources Management (6324)

For AMP Students Only

Presents an overview of public sector resource management concepts, policies, and policy constituencies, focusing on the application of these concepts and policies as mechanisms of modern governance. The course focuses on the application and interaction of financial, information, and human resources to achieve legislative and policy goals and accomplish agency missions. Students explore the entire life cycle of resource management, from the expression of political purpose in legislation and policy, through governance and program implementation, to managing program performance and assessing program effectiveness. Legislation and policies for managing financial, information, and human resources in public organizations are examined against a backdrop of the dynamic political, economic, technological, and societal interactions that are changing governments worldwide.

Learning Outcomes: Students will be able to illustrate linkages between political purpose, policy, governance, resources and their management, and achieving results in political, organizational, and functional contexts; explain the substance of resource management policies for technological, fiscal, human, and information resources, and demonstrate resource integration approaches for achieving policy objectives and organizational mission success; and assess the impacts of dynamic domestic and international political, economic, and societal interactions on implementing mission-oriented programs, and on integrating resources to ensure successful agency outcomes and achieve political purposes.

RIA

Risk Management, Internal Controls, and Auditing for Leaders (6608)

For CFO Certificate students only

This course presents a strategic understanding of risk management, internal controls, and auditing as they relate to the functions and responsibilities within the CFO and audit communities. This course examines how effective leadership can enhance efficiency, effectiveness, accountability, and transparency of an organization to include federal, state, and local governments. The primary focus is on the importance of identifying and assessing risks, describing and improving internal controls techniques and practices, and evaluating and recommending audit management strategies. The course includes practical discussions to illustrate how these processes can be integrated and leveraged to solve problems, make informed decisions, and minimize compliance costs.

Learning Outcomes: Students will be able to articulate the importance of risk management and demonstrate how risk management techniques can be used in their organizations to improve overall effectiveness and address fiscal and operational challenges that exist in the public sector; describe and apply internal controls techniques for assessing financial, as well as, program operations; describe the audit process and the key roles and responsibilities of auditors; recommend techniques used to effectively manage the audit process, which can result in improved working relationships between auditors and auditees; and to identify the key elements of effective risk management, internal controls, and auditing processes and show how these components can be integrated and leveraged to add value to the organization.

SAL

Software Acquisition Leadership (6410)

Recommended: ITA

This course provides comprehensive insight into the risks and issues associated with developing and implementing complex software systems. Students examine the risks, problems and issues that challenge large or complex software acquisition, integration, or development efforts, and evaluate strategies, methods, and tools to achieve successful program outcomes. Specific areas of focus include software development methods, tools and best practices, software-unique testing and architecture issues, and software assurance challenges and issues.

Learning Outcomes: Students will be able to evaluate anticipated challenges and risks of software acquisition, integration, and development projects, and create appropriate and effective strategies to manage them.

SCL

Strategic Communication for Government Leaders (6322)

The course begins with communication theories and applications and ends with the role of strategic communication for government leaders. It explores the pivotal role of communication in achieving organizational and national strategies. The course investigates the psychological, cultural, political, and technological factors that mediate communications for national and international audiences so as to influence key decision makers, critical audiences, and general populations. Students analyze how government strategic leaders can be strengthened as producers and consumers of public information through social influence, persuasion and propaganda, public opinion and mass political behavior, crisis communications, media relations, communication law, policy and ethics, and the role of advanced telecommunication technologies.

Learning Outcomes: Students will be able to assess how strategic communication shapes public perceptions and beliefs at all levels, from domestic perceptions to international attitudes; and to develop and employ strategic communication processes and plans consonant with current communications theory that support their agency's mission and national security strategy.

SEC

Cyber Security for Information Leaders (6201)

This course explores concepts and practices of defending the modern net-centric computer and communications environment. The course covers the 10 domains of the Certified Information System Security Professional (CISSP®) Common Body of Knowledge (CBK®). It covers a wide range of technical issues and current topics including basics of network security; threats, vulnerabilities, and risks; network vulnerability assessment; firewalls and intrusion detection; transmission security and TEMPEST; operating system security; web security; encryption and key management; physical and personnel security; incident handling and forensics; authentication, access control, and biometrics; wireless security; virtual/3D Worlds; and emerging network security technologies such as radio frequency identification (RFID) and supervisory control and data acquisition (SCADA) security. The course also defines the role of all personnel in promoting security awareness.

Learning Outcomes: Students will be able to evaluate the cyber-security posture of an organization to determine adequate people, processes, and technology security.

SLP

Strategic Leader Theory and Practice (6325)

For AMP Students Only

Focuses on the competencies of strategic leaders in theory and in practice across a variety of contemporary defense, government, and private sector organizations. Students will evaluate, reflect upon, and refine their strategic leader strategies for leading and building effective organizations. They will examine a diversity of organizations to draw insights that they can apply to their organizations and their own practice of leadership. Key components of the course include individual awareness, team problem solving, and studies with and about exemplar organizational leaders.

Learning Outcomes: Students will be able to develop enterprise strategic leader strategies; demonstrate critical introspection, communication, research, teamwork, and strategic thinking; integrate leadership theory and best practices into their personal leadership practice; and, synthesize and integrate the total AMP experience into actionable steps for organizational enhancement.

SPA

Privacy Rights and Civil Liberties (6231)

This course focuses on protecting personal information while exploiting new technologies, implementing cross-agency information sharing, and improving the processes of government and service to the public. The rights, needs and perspective of the citizen are discussed with regard to public policy and legal frameworks. Best business practices, such as using Privacy Impact Assessments (PIAs) and identity management techniques, are explored as mechanisms for evaluating and dealing with privacy issues. The course enables managers to deal with the privacy concerns of citizens and stakeholders when implementing new systems and technology and transforming agency processes. Students identify leadership and management approaches to ensure appropriate information access and privacy protection.

Learning Outcomes: Students will be able to recommend appropriate protection strategies, tools, and methods for processing and sharing private information; and develop policies to manage privacy in government initiatives.

STA

Enterprise Solutions Architecture and Transition Planning for Architecture (6440)

Prerequisite: Successful completion of Level II EA certificate courses. Students will be required to install a provided EA modeling repository tool on a non-iCollege computer. This course prepares the senior or chief architect to collaborate with the solutions architect(s) to develop target enterprise-wide technology architecture and solution strategies that complement and enable the target enterprise business environment. Students examine a general target technology framework and assess alternative technology architecture end-states for enterprise–wide service oriented architecture and capabilities-based architecture. For each general design end-state, alternative criteria are considered to provide alternative technical designs. Students examine strategies for developing a security architecture. The course concludes with a consideration of alternative legacy migration and transition strategies.

Learning Outcomes: Students will be able to design enterprise-scale target solution architectures and develop alternative transition plans as a function of target end-state of the EA architecture.

TCC

Terrorism and Crime in Cyberspace (6215)

This course explores the nature of conflict in the cyber realm by focusing on two major Internet-based threats to U.S. national security: cyber terrorism and cyber crime. The course examines who is undertaking these cyber activities, what techniques they use, and what countermeasures can be adopted to mitigate their impact. The course provides a risk management framework to help information leaders leverage the benefits of Internet technologies while minimizing the risks that such technologies pose to their organizations.

Learning Outcomes: Students will be able to assess the risks posed by cyber terrorism and cyber crime to U.S. national security in general, and to their specific organizations in particular; and evaluate the benefits and costs of different countermeasures that could be used to mitigate those risks.

WGV

Web-Enabled Government: Facilitating Collaboration and Transparency (6435)

This course explores the capabilities, selection, and application of new and emerging web technologies to enable more creative, collaborative, and transparent government. The course examines and assesses the use of current and emerging web technologies and best practices of significant government interest, e.g., cloud computing, social media and networking, geographic information services technology, and security. Students consider web technology evaluation criteria, methodologies, and risks to enable them to adapt the evaluation criteria and apply selected web technologies within and/or across government.

Learning Outcomes: Students will be able to evaluate the benefits and risks of current and emerging web technologies; analyze the strategic advantages and disadvantages of each; and choose and implement web technologies that increase engagement, collaboration, and transparency within and/or across government.

Academic Partners

The NDU iCollege continues to form academic partnerships with regionally accredited universities across the United States, mainly signing Memoranda of Understanding (MOUs) with schools that are Centers of Academic Excellence (CAEs) in Information Assurance Education. Graduates from the college's many certificate programs can apply to a number of partner institutions for completion of a Master's or Doctoral/PhD Degree. There are many degree choices for NDU iCollege graduates at the partner institutions. Academic partners accept 9, 12, or 15 graduate semester credits depending on which certificate program was completed at the NDU iCollege. Many academic partners provide full-time, part-time, and online educational opportunities.

As of catalog print date, there are more than 40 current NDU iCollege academic partners, which are listed below. Please refer to the NDU iCollege website partnership matrix at: http://www.ndu.edu/iCollege/network/ntwk_list1.html for more details on the exact number of credits and point of contacts at each partner institution. Several schools updated their agreements over the previous year to include new degrees and acceptance of more NDU iCollege certificates. Please check the website often for changes and additions. IA Scholarship Program (IASP) students may apply to schools and degrees designated as "IASP-qualified" in the partner matrix.

Questions about the partnership program should be directed to Patricia Coopersmith, Director of Outreach & International Relations, at coopersmithp@ndu.edu, 202-685-2117. Specific questions about degree programs, admission requirements, or remaining courses should be directed to the academic partner institution representative.

Current NDU iCollege Academic Partners

Auburn (AL)
Cal State San Bernardino (CA)
Capitol College (MD)
Central Michigan University (MI)
Clemson University (SC)
East Carolina University (NC)
Eastern Michigan University (MI)
Florida Institute of Technology (FL)
Fort Hays State University (KS)
George Mason University (VA)
Georgetown University (DC)
Illinois Institute of Technology (IL)
James Madison University (VA)
Johns Hopkins University (MD)
Mississippi State University (MS)
Missouri University of Science & Technology (MO)
New Jersey City University (NJ)
New Mexico Tech (NM)
Northeastern University (MA)
Norwich (VT)
NYU - Poly (NY)
Pace University (NY)
Regis University (CO)
Rochester Institute of Technology (NY)
San Diego State University (CA)
Southern Methodist University (TX)
Syracuse University (NY and DC)
Texas A&M (TX)
Towson University (MD)
University of Arkansas at Little Rock (AR)
University of Dallas (TX)
University of Detroit Mercy (MI)
University of Illinois at Springfield (IL)
University of Illinois at Urbana Champaign (IL)
University of Maryland Baltimore County (MD)
University of Maryland University College (MD)
University of Nebraska at Omaha (NE)
University of North Carolina at Charlotte (NC)
University of Pittsburgh (PA)
University of Texas at San Antonio (TX)
University of Tulsa (OK)Walsh College (MI)

NDU iCollege Awards

2011 Recognition:

- Federal 100 Award from Federal Computer Week, Dr. Robert Childs
- AFCEA Meritorious Award for Excellence in Information Technology, Patty Coopersmith
- Finalist, Women in Technology Leadership Award, Education IT, LTC Veronica Wendt
- 2011 Educator Award from the Association of Government Accountants (AGA), Ricardo Aguilera and Gary Maupin

2010 Recognition:

- Federal 100 Award from Federal Computer Week, Dr. Robert Childs
- Finalist, eLearning Age Awards, Excellence in Online Learning Content, Dr. Cathy Downes for MAC course
- Government Information Security Leadership Awards (GISLAs), Mark Duke for AII class
- AFFIRM Awards, Leadership in Service to the Government IT Community, Dr. Robert Childs
- Finalist, Women in Technology Awards/Government, Dr. Paulette Robinson
- AFCEA Meritorious Award for Excellence in Information Technology, Dr. Mawan Jamal
- AFCEA Bethesda Chapter, Excellence in Human Capital and Workforce Industries, Dr. Robert Childs

2000-2009 Recognition:

- 2009 Federal 100 Award from Federal Computer Week, Dr. Robert Childs
- Excellence in IT Award from AFCEA, Dr. Robert Childs
- 2009 Eagle Award from Federal Government Distance Learning Association
- Intergovernmental Solutions/Management of Change Award (finalist), American Council for Technology
- 2009 Rising Star Award from 1105 Government Information Group, Dr. Mawan Jamal
- Finalist, SC Magazine Awards, Best Professional Certificate Programs
- Best Practice Awards in Corporate/College Partnerships from CUX
- 2004 Tele-work in the Federal Government Leadership Award
- 2003 Golden Link Award for partnering with industry from AFCEA
- Excellence in Corporate Education Award from London Financial Times
- 2002 Federal 100 Award from Federal Computer Week, Dr. Robert Childs
- 2001 Federal 100 Award from Federal Computer Week, Dr. Robert Childs

Patty Coopersmith, Director of Outreach and International Relations, NDU iCollege, talks with conference participants at the NDU iCollege booth, 2010 Regional Collaboration in Cyber Security Conference held in Singapore

Admissions, Registration, and Program Completion Policies

Admission

National Defense University (NDU) iCollege courses are available to Department of Defense (DoD) civilian employees and military officers, eligible federal government civilian agency employees, non-Federal Government employees (i.e., state, local, and tribal governments), and private sector employees.

International students (non-U.S. citizens) are also eligible to attend the NDU iCollege and must apply through the appropriate Security Assistance Training Field Activity (SATFA) country program manager.

Minimum Admission Eligibility Criteria

U.S. Government Affiliation	Federal Government civilian employees, military officers, non-federal government employees (state, local, and tribal governments), and private sector employees.
Education	All applicants must possess a Bachelor's degree from a regionally accredited U.S. institution or the equivalent from a foreign institution. **Additional for M.S. Degree Program** The minimum grade point average considered for admission is a 3.0 on a 4.0 scale for all previous undergraduate work. In cases where the undergraduate GPA is below 3.0 a cumulative GPA of 3.5 in 12 or more graduate credit hours (from the NDU icollege or other graduate programs) may be used to determine eligibility.
Pay Grade/Rank, Experience	Varies by NDU iCollege program
Certificate Programs and Advanced Management Program (AMP) (includes PD)	Federal civil service pay grade of GS/GM-12 or equivalent/military officer rank of O- 4 or above. Non-federal employees, to include state and local government, must be of an equivalent grade. Private sector employees must be of an equivalent grade and work in a field relevant to the iCollege curriculum. Private sector employees must provide a resumé detailing last 5 years of employment history as part of their application.
CFO Leadership Certificate Program (CFO)	Federal civil service pay grade of GS/GM-14 or equivalent/military officer rank of O-5 or above. (High performing GS/GM-13s and O-4s are also eligible on a case by case basis.) Non-federal employees, to include state and local government, must be of an equivalent grade. Private sector employees must be of an equivalent grade and work in a field relevant to the iCollege curriculum. Private sector employees must provide a resumé detailing last 5 years of employment history. Documented Knowledge of Financial Management, Experience: Undergraduate or Graduate degree in finance or business field, CPA, CGFM or CDFM or three years of federal financial management experience is required.
Masters of Science (M.S.)	Federal civil service pay grade of GS/GM-12 or equivalent/military officer rank of O- 4 or above. Non-federal employees, to include state and local government, must be of an equivalent grade. Private sector employees must be of an equivalent grade and work in a field relevant to the iCollege curriculum. Private sector employees must provide a resumé detailing last 5 years of employment history as part of their application.
English Language Proficiency	ECL or TOEFL scores (as necessary). Applicants whose native language is not English are required to demonstrate their English proficiency by passing an English comprehension test with either an ECL of 85 or TOEFL of 213 (computer based), unless their university degree is from an institution where the curriculum was taught exclusively in English. Contact the NDU iCollege Office of Student Services for further details.

Application Requirements

Advanced Management Program	• Application for Admission • Resumé • Nomination Letter
Dual Admission (M.S. Degree/ AMP)	• Students interested in seeking dual admission to the AMP and the GIL M.S. degree program must do so at the time of AMP program admission. The following additional documents are required (see section on **Required Documents for M.S. Program** for more information) • One supervisory letter of recommendation • One professional letter of recommendation • Official transcript(s) from a regionally accredited U.S. institution or the equivalent from a foreign institution.
Certificate and Professional Development Programs (excluding AMP and CFO)	• Application for Admission • Employer Verification and Sponsorship form • Resumé (Private Sector Applicants Only)
CFO Leadership Certificate Program	• Application for Admission • Employer Verification for the CFO Leadership Program • Resumé (Private Sector Applicants Only)
Government Information Leadership M.S. Program	The Government Information Leadership (GIL) Master of Science Degree is a selective degree program. Applicants must include all of the required documents listed below in the same application packet to be considered for admission. • Application for Admission • Employer Verification and Sponsorship form for the GIL Master of Science Degree Program • Resumé • One supervisory letter of recommendation • One professional letter of recommendation • Official transcript(s) from a regionally accredited U.S. institution or the equivalent from a foreign institution.

"Course material was absolutely top notch in content. Comprehensive, meaningful and relevant. It was clear that the material is contemporary and carefully selected and that it was relevant to all students. Logistics, security, IT were all covered really well." -iCollege Student

Change in Eligibility: The NDU iCollege will periodically review eligibility of active students. If a student's eligibility changes (employer, pay grade, rank, etc.), the student must notify the NDU iCollege Office of Student Services (OSS). In cases where course credit is earned after eligibility ceases, course credit may be revoked and/or the student may be held liable for tuition fees. NDU iCollege Office of Student Services (iCollegeOSS@ndu.edu; Fax: 202-685-4860).

Required Documents for Program Admission

Detailed application instructions, forms and templates are available online from the NDU iCollege's website: www.ndu.edu/icollege/application.

Course Registration

Once accepted to the NDU iCollege, students in the Master of Science degree program, the Graduate Certificate programs, or the Professional Development program will be assigned an account, username, and password to be used to self-register in the desired courses using the College's online student information system. (Detailed instructions are sent at time of admission.) Course descriptions and offering dates/formats are available on the college's website.

In consultation with the Advanced Management Program (AMP) Director, AMP students will be registered automatically in the courses necessary for completion of their program.

Confirmation of Course Registration
Students may confirm successful course registration by viewing their course schedule online. A course acceptance notice will automatically be sent to students who successfully register for a course. The NDU iCollege may send additional reminders and attendance confirmation requests prior to the course start date. Students should promptly respond to requests for information.

Multiple Registrations Policy

Students may register as follows:

1. One Distributed Learning (DL) offering per term (Fall, Spring, Summer) OR
2. One DL offering and one resident offering per DL term (Fall, Spring, Summer) OR
3. One or more resident offerings when instructional periods do not overlap (i.e. the instructional period in the first three weeks of the course).

Permission to register for more than one online (DL) course per term (Fall, Spring, Summer) may be granted by requesting an exception to policy (maximum 2 courses per session). Requests must be submitted to the NDU iCollege Office of Student Services in writing (iCollegeOSS@ndu.edu; Fax: 202-685-4860) no later than 2 weeks prior to the course start date. Note: A student who is granted permission but fails to complete both courses successfully may not be considered for concurrent registration in the future.

Dropping a Course
If prior to the Course Start Date (CSD), students are unable to attend a course, they must drop the course using the NDU iCollege's student information system.

Students who drop a course on or after the Course Start Date (CSD) but before 25 percent of the course is completed will receive an academic grade of W (withdrawal).

Students who drop a course after 25 percent of the course is completed will receive a grade of F, unless he or she can provide documented evidence of extenuating circumstances (e.g. hospitalization, deployment to combat zone).

(See Academic Policies-Grading section for additional information.)

Tuition

Since the NDU iCollege is a U.S. Department of Defense (DoD) institution, there are no tuition fees for DoD civilian and military employees for NDU iCollege courses or academic programs. This includes all course offerings and the Advanced Management Program, but may not include special offerings such as executive or special seminars.

Fiscal Year 2011 - 2012 Tuition*		
Employer Category	Course	Advanced Management Program (AMP)
DOD civilian, Active U.S. Military & Uniformed Services, Active Military Reserve or National Guard	None	None
Non-DOD civilian, State and Local government	$1125	$10750
Private Sector	$2050	$16900
*Fiscal Year 2011-2012: October 1, 2011 to September 30, 2012.		

Note: Military members in the Reserve or National Guard may apply for admission and tuition waivers based on their 'Fulltime Reserve or National Guard Duty Status' (i.e., drilling status). Documentation must be provided prior to attendance or the student will be liable for the full tuition owed. Contact the NDU iCollege Office of Student Services for detailed instructions.

Payment Instructions

Students should make all payments for courses no later than the first day of the offering. If payment is not received, the account is considered delinquent and the student may not be admitted to the course or allowed to attend future courses until his or her account is cleared.

The NDU iCollege cannot accept cash payments. Valid forms of payment are credit card, check, electronic funds transfer, and Military Interdepartmental Purchase Request (MIPR). Detailed instructions for submitting payment are provided to the student by e-mail and on the student's invoice when the student is accepted into a course.

Program Completion

Program Completion Time Limit

Master of Science (M.S.) Degree Program: All coursework applied toward a M.S. Degree must be completed within seven (7) years of graduation.

Graduate Certificate Programs: All coursework applied toward a certificate must be completed within four (4) years graduation.

Students must successfully complete at least one course every 12 months to maintain active status in NDU iCollege programs. An approved leave of absence will stop the student's program completion timeline (see section General Policies- Leave-of-Absence).

Graduation Diplomas and Certificates (credentials)

Master's degree diplomas and program certificates are prepared annually for graduation exercises. Master's degree diplomas and ceremonial certificates are mailed to the home address of students who do not attend the ceremonies. Students are responsible for maintaining current mailing addresses in the student information system to ensure delivery is not delayed.

Completion Procedures

It is the student's responsibility to meet all program requirements and to timely apply for graduation. Students of the NDU iCollege who have completed program requirements must submit the "Application for Graduation" via email directly to the NDU iCollege.

To officially graduate from a program, the student must:

1. Be admitted in the academic program(s) he or she intends to complete.
2. Complete all course requirements. (The student may use the program requirements of the catalog in force at the time of his or her initial acceptance, or the student may choose to fulfill the requirements of the current catalog.)
3. Complete and submit the "Application for Graduation" form. A passing grade for all applicable courses must be posted to the student's transcript to be eligible for program completion. An ineligible applicant will not be processed for completion and the student must reapply when all coursework has been successfully completed and posted.

If there are questions regarding the requirements for graduation, contact the NDU iCollege's academic advisor.

After the student's transcript has been validated, the certificate name and completion date will be noted on the student's official transcript and the Office of Student Services will send a 'program completion letter' signed by the NDU iCollege Chancellor to the student's home address on record. The date noted in the program completion letter or official transcript is the official completion date. Dates on certificates awarded at the College's commencement ceremony reflect the ceremony date and should not be used for reporting purposes.

Commencement Exercises

Master of Science (M.S.) Degree Program: Master of Science in Government Information Leadership degree candidates attend the National Defense University commencement ceremony held in early June of each year.

Graduate Certificate Programs: The NDU iCollege certificate commencement is traditionally scheduled for the last week in April. (Check the NDU iCollege website for exact date and time.) Those who complete certificate programs throughout the year are eligible to attend.

The Office of Student Services will contact all known and potential graduates at the students' preferred e-mail address as shown in the student information system approximately eight weeks prior to commencement exercises. This e-mail message will provide detailed timelines and procedures that students must follow to be included in the commencement planning.

Students who are attempting to complete their programs within two months prior to commencement exercises in April are advised to work closely with their advisor and course instructors to ensure they meet requirements to participate in commencement exercises.

Records Maintenance

The NDU iCollege maintains hard copies and electronic records as required for all prospective, current, and past students. Current students are responsible for ensuring their current biographic and demographic information are correct at all times in the student information system to assist the NDU iCollege in communicating expeditiously with students, and to meet Federal and Department of Defense directives and reporting requirements. Students are encouraged to notify the NDU iCollege Office of Student Services of any changes to their contact information (e.g., telephone number, email or physical address, etc.) for future correspondence.

Dr. Mary McCully , Dean of Faculty and Academic Programs, NDU iCollege

Transcripts

Student academic records are confidential and may be released only with the student's written authorization and signature, in accordance with the Privacy Act of 1974.

Two types of transcripts are available from the National Defense University, as described below. NDU iCollege student grade point averages are calculated for use internal to the NDU iCollege and will not appear on NDU transcripts.

Official Transcripts: An official transcript is a certified copy of student's permanent academic record that displays all courses taken at NDU and includes all grades received and is issued by the University Registrar. Official university transcripts are printed on purple SCRIP-SAFE security paper with the name of the university printed in white typed across the face of the document and do not require a raised seal. When photocopied, the word COPY appears prominently across the face of the entire document

Unofficial Transcripts: An unofficial transcript is an uncertified copy of the student's academic record. Unofficial university transcripts display all courses taken at NDU and include all grades received, but do not include the university seal, the signature of the registrar, or the name of the university.

Transcript Request Process: Students must request official and unofficial transcripts through the University Registrar's Office. The NDU iCollege staff cannot request or print official NDU transcripts for a student. Transcripts may be obtained by completing the Transcript Request Form (http://www.ndu.edu/AA/Transcript_Request_Form.pdf) and emailing, faxing or mailing the request to the University Registrar's Office at:

The National Defense University
University Registrar's Office (URO)
300 5th Avenue SW, Bldg 62
Washington, D.C. 20319-5066
Phone: (202) 685-2128 (DSN: 325)
Fax: (202) 685-3920 (DSN: 325)
University-Registrar@ndu.edu

Please note that unofficial transcripts cannot be mailed or emailed, and must be faxed or picked up in person.

The excellent education and networking opportunities I received while attending classes at the National Defense University (NDU iCollege) enabled me to earn certificates in Cyber Security, Information Technology Program Management and Chief Information Officer disciplines. The most important aspect of this educational opportunity was exposure to current and practical global issues--giving me the edge to affect change in the workplace and lead the tomorrow's generation.

- iCollege graduate

General and Academic Policies

Admission to Multiple Academic Programs

Students may apply for, and be admitted to, more than one NDU iCollege academic program at a time. However, students may only pursue and be awarded one area of concentration in the Government Information Leadership Master of Science Degree Program.

Applying Coursework Earned Prior to Program Admission

Graduate Certificate Program Participants. If a student has completed NDU iCollege coursework under another program, the student may apply eligible courses to another certificate program. Eligible courses are those that meet a program's requirements. Courses taken for Professional Development (PD) are not applicable. All coursework applied toward a certificate must be completed within the previous four years.

Master of Science Program Participants. Subject to the graduation time limit requirements, a student may use all NDU iCollege classes passed with a grade of B or higher toward attaining the M.S. degree. No courses from other institutions are accepted for transfer. Courses taken for Professional Development (PD) are not eligible. All coursework applied toward a M.S. degree must be completed within the previous seven years.

Program Actions

Leave of Absence

Students may apply for a leave of absence due to exceptional circumstances by submitting a written request to NDU iCollege Office of Student Services. The letter should provide a detailed explanation of the circumstances leading to the request and a justification of the time requested. Requests for a leave of absence may be made for up to one academic year. An approved leave of absence will stop the student's program completion timeline. Requests should be e-mailed to iCollegeOSS@ndu.edu. Confirmation will be provided by e-mail.

Program Withdrawal

Students who wish to end their participation in an NDU iCollege program may submit a written request to the NDU iCollege Office of Student Services. The request should state the student's name, e-mail address (if different than on record), program(s) from which the student wishes to withdraw, and a brief justification statement. Requests should be e-mailed to iCollegeOSS@ndu.edu. Confirmation of withdrawal will be provided by e-mail.

Dismissal

The NDU iCollege may dismiss students from a program for a number of reasons that include, but are not limited to, unsatisfactory academic progress performance (including not taking one course every 12 months) and/ or upon the decision of the Academic Review Board.

Reinstatement

Students who wish to request reinstatement must reapply. The NDU iCollege may grant reinstatement to a program on a case-by-case basis. Once eligibility is reviewed, it will be determined which previous courses, if any, may apply to the program of study.

Requirements for Continued Enrollment

Students enrolled at the NDU iCollege must maintain satisfactory progress by completing at least one course every 12 months and maintaining a 3.0 cumulative GPA. Students are expected to achieve a satisfactory grade (A, A-, B+, B) in all coursework attempted for academic credit.

Students will be automatically placed on probation upon receiving one (1) course grade of F and/or whenever his or her cumulative GPA falls below 3.0. A student on probation must attend a mandatory counseling session with their advisor, and if applicable, raise the GPA to a 3.0 at a timeline or credit load defined by the NDU iCollege Office of the Dean of Academic Programs. Students who receive a second course grade of F and/or who fail to raise their GPA within the prescribed timeline or credit load will be dismissed from the NDU iCollege.

Attendance Policy

Students are expected to participate in all scheduled class sessions and activities as a prerequisite to the award of the course certificate. The College will not issue a course certificate if a student misses more than five percent of the class time or if the student misses critical portions of the course.

Absence from class activities degrades the continuity and effectiveness of the educational process for all involved. Accordingly, absences may be authorized only under the most extenuating circumstances. Students are responsible for any course work missed.

The Course Manager must approve all absences. In cases requiring emergency absence for medical or other serious reasons, authorization should be obtained in advance of the absence whenever possible.

Academic Policies

Student Assessment

All NDU iCollege students must demonstrate a successful level of mastery of the intended learning outcomes of each course. Faculty members formally assess student achievement on learning outcomes as detailed in course assessment plans and provide detailed feedback to students on their performance as an essential component of the learning process. Faculty members develop an assessment plan documenting the proposed assessment techniques they will use and grading guidelines for all assignments and/or instruments (paper, project, presentation, participation). At the NDU iCollege, end-of-course assessments require students to apply the material through written papers or presentations based on their real-world environments (usually their own agencies or units). Final end-of-course assessments submitted for a grade cannot be rewritten or resubmitted.

Grading

The following letter grades and their achievement equivalents are used by the NDU iCollege to evaluate a student's performance in a course and in a program. Grade points corresponding to each letter grade determine a student's academic average and eligibility to graduate. Each grade, A through F, has a specific grade point value (see table below). Master of Science and Graduate Certificate students must maintain a grade point average (GPA) of at least 3.0 to graduate.

GPA is obtained by dividing the total number of letter grade credits taken in the graduate program into the total number of grade points earned in the graduate program. Only letter grades with GPA values will be used in computing the GPA. A student may repeat any course in which a grade of C or lower is received. The grade earned by repeating a course is used for computing the GPA in lieu of the grade originally earned, although the original grade will remain on the transcript. GPAs will not appear on NDU transcripts.

C Grade: Only one grade of C may be used to fulfill program requirements. The grade of C cannot be used to fulfill requirements for the Master of Science Capstone (CAP) course. C grades may not be transferrable to other Universities' graduate level programs.

F Grade: When a grade of F is assigned, the student will not receive academic credit for the course and the GPA value of 0.0 will be calculated. This grade is used when:

- A student fails to meet minimum academic requirements
- A student chooses to drop from a course after 25 percent of the course is completed without documentation of extenuating circumstances

Other/Non-GPA Annotations

Incomplete (I): This grade is assigned to students who, due to unusual and extenuating circumstances (e.g. serious illness, deployment to combat zone), are granted an extension to complete the academic requirements (usually a final paper and/or project) past the course deadline. The requesting student must have satisfactorily met the attendance/participation

Grade Scale

GPA Grades (Academic Credit is Earned)

Letter Grade	GPA Value	Description
A	4.0	Exceptional Quality
A-	3.7	Very High Quality
B+	3.3	High Quality
B	3.0	Average Quality
C	2.0	Below Expected Quality
F	0.0	Unsatisfactory Quality

Other/Non GPA Annotations/Actions (Academic Credit is Not Earned)

I	Incomplete
PD	Professional Development
W	Withdrawal

requirements for the course and request an extension in writing to the Offering Leader prior to the assignment deadline. The written request must provide acceptable reasons for an extension and a proposed deadline for submission. The Offering Leader will deny or approve the request in writing. Approved extensions are not to exceed one week. Extensions which exceed one week must be approved by the Office of the Dean of Academic Programs.

Professional Development (PD): This grade is assigned to students who elect to take a course for professional development and successfully complete requirements except the final assessment. Students do not receive academic credit for professional development courses. Students must retake courses for credit if they want to apply them to a program.

Course Withdrawal (W): Students who drop a course on or after the Course Start Date (CSD) but before 25 percent of the course is completed will receive an academic grade of W. The student must submit the request to withdraw in writing to the Office of Student Services. A grade of W also can be assigned by the faculty or the Office of Student Services for administrative purposes (such as unacceptable performance during the Preparation Week of an eResidence course). Students who drop a course after 25 percent of the course is completed will receive a grade of F, unless he or she can provide documented evidence of unusual and extenuating circumstances (e.g. serious illness, deployment to combat zone).

Academic Integrity

The NDU iCollege has a zero tolerance policy toward plagiarism and other breaches of academic integrity, and will enforce the National Defense University Statement on Academic Integrity as summarized below. Students should consult the NDU website at http://www.ndu.edu/aa/policies.cfm for the complete and/or most current NDU academic integrity policy.

Statement On Academic Integrity

NDU shall always foster and promote a culture of trust, honesty, and ethical conduct.
This statement on academic integrity supports the above guiding principle and applies to all components of the National Defense University. The purpose of this broad university policy is to establish a clear statement for zero tolerance for academic dishonesty and to promote consistent treatment of similar cases across the University on academic integrity and the integrity of the institution. This document should not be interpreted to limit the authority of the University President or the Vice President for Academic Affairs. This policy includes two key areas: academic integrity as it applies to students and participants at National Defense University; and academic integrity as it applies to assigned faculty and staff.

Breaches of Academic Integrity

Breaches of academic integrity are not tolerated. Breaches include, but is not limited to: falsification of professional and academic credentials; obtaining or giving aid on an examination; having unauthorized prior knowledge of an examination; doing work or assisting another student to do work without prior authority; unauthorized collaboration; multiple submissions; and plagiarism.

Falsification of professional and academic credentials: Students are required to provide accurate and documentable information on their educational and professional background. If a student is admitted to the University with false credentials, he or she will be sanctioned.

Unauthorized collaboration is defined as students working together on an assignment for academic credit when such collaboration is not authorized in the syllabus or by the instructor.

Multiple submissions are instances in which students submit papers or work (whole or multiple paragraphs) that were or are currently being submitted for academic credit to other courses within NDU or at other institutions. Such work may not be submitted at the National Defense University without prior written approval by both the National Defense University professor/instructor and approval of the other institution.

Plagiarism is the unauthorized use of intellectual work of another person without providing proper credit to the author. While most commonly associated with writing, all types of scholarly work, including computer code, speeches, slides, music, scientific data and analysis, and electronic publications are not to be plagiarized. Plagiarism may be more explicitly defined as:

- Using another person's exact words without quotation marks and a footnote/endnote.
- Paraphrasing another person's words without a footnote/endnote.
- Using another person's ideas without giving credit by means of a footnote/endnote.
- Using information from the web without giving credit by means of a footnote/endnote. (For example: If a student/professor/instructor/staff member enrolled or assigned to NDU copies a section of material from a source located on the internet (such as

Wikipedia) into a paper/article/book, even if that material is not copyrighted, that section must be properly cited to show that the original material was not the student's).

To remind students of possible breaches of academic integrity, they are encouraged to submit their papers and assessments for review by plagiarism detection software prior to turning the products in for grading.

Sanctions for Breaches of Academic Integrity

Sanctions for breaching the academic integrity standards include but are not limited to: disenrollment, suspension, denial or revocation of degrees or diplomas, a grade of no credit with a transcript notation of "academic dishonesty;" rejection of the work submitted for credit, a letter of admonishment, or other administrative sanctions. Additionally, members of the United States military may be subject to non-judicial punishment or court-martial under the Uniformed Code of Military Justice. The authority for decisions and actions rests at the NDU iCollege.

Academic Review Board

The NDU iCollege Academic Review Board is responsible for reviewing cases of student performance that include breaches of the College's academic integrity policy.

The student will be notified by e-mail and U.S. mail that he or she has been referred to the Academic Review Board. The communication will include a summary of the reason for the referral and invite the student to appear before the Academic Review Board.

When a student's work is referred to the Academic Review Board, his or her record will be placed on "Academic Hold" status. All actions affecting their coursework, including grading, will be suspended pending outcome of the Academic Review Board's inquiry.

Professor Jay Holcomb, leads a discussion in one of the iLabs, NDU iCollege

Faculty & Administration

LEADERSHIP

Robert D. Childs
Chancellor;
B.S., Grove City College;
M.A.T., Duke University;
Ed.D., University of Denver;
Air Command and Staff College;
National War College, National Defense University;
Fuqua Business School, Duke University.

Mary S. McCully
Dean of Faculty and Academic Programs;
B.S., Marygrove College;
M.S., Air Force Institute of Technology;
M.A., University of Northern Colorado;
M.Ed., Marymount University;
Air War College;
Industrial College of the Armed Forces, National Defense University;
Ph.D., Arizona State University;
Harvard Senior Executive Fellow.

Russell E. Quirici
Dean of Students and Administration;
B.S., United States Military Academy;
M.A., The Pennsylvania State University;
M.S., National War College, National Defense University.

Paulette Robinson
Associate Dean for Teaching, Learning and Technology;
B.A., University of Hawaii;
M.A., University of Hawaii;
M.N.A., University of San Francisco;
Ph.D., University of Maryland.

Cassandra C. Lewis
Assistant Dean for Curriculum;
B.A., University at Buffalo;
M.A., Boston College;
Ph.D., University of Maryland.

John T. Christian
Chair, Information Strategies Department;
B.A., University of Virginia;
M.A., Ph.D., Vanderbilt University.

Gilliam E. Duvall
Chair, Cyber Integration and Information Operations Department;
B.S., Purdue University;
M.S., The Naval Postgraduate School.

Andrew P. Gravatt
Chair, Systems and Technology Department;
B.S., University of Maryland;
M.S., The Johns Hopkins University Whiting School of Engineering.

Todd Holmes
Chair, Chief Financial Officer Academy;
B.S., The Citadel;
M.B.A., Golden Gate University;
D.A., George Mason University.

Elizabeth A. McDaniel
Distinguished Faculty;
B.A., University of Florida;
M.A., Barry University;
Ph.D., University of Miami.

Patricia Coopersmith
Director of Outreach and International Relations;
B.S., The Pennsylvania State University;
M.B.A., Augusta State University.

Gerry Gingrich,
Director, Advanced Management Program;
B.S., University of North Carolina;
M.S., Ph.D., University of Maryland;
Post-Doctoral Fellowship, University of Minnesota.

Michael Piller
Director of Academic Computing and Laboratories;
B.S., Wright State University;
M.A., Ph.D., Catholic University of America.

Donna Powers
Director of Academic Support;
B.S., University of Washington;
M.A., Golden Gate University.

FACULTY

Ricardo Aguilera
Chief Financial Officer Academy;
B.A., New York University;
M.A., The George Washington University.

Jay Alden
Information Strategies Department;
B.S., Long Island University;
M.S., Hofstra University;
Ph.D., Hofstra University.

Michael Bartlett
B.B.A Georgia State University
M.S. Central Michigan State University

William S. (Stan) Boddie
Systems and Technology Department;
B.A., Saint Leo College;
M.A., Webster University;
M.S., George Mason University;
Ph.D., The University of Phoenix.

Mary Cole Carroll
Cyber Integration and Information Operations Department;
B.A., Metropolitan State College of Denver;
M.B.A., The George Washington University;
M.S., Industrial College of the Armed Forces, National Defense University;
J.D., Georgetown University Law Center.

Richard B. Cespiva
Cyber Integration and Information Operations Department;
B.S., Loyola University;
M.S., American Intercontinental University.

James F. Churbuck
Cyber Integration and Information Operations Department;
B.S., United States Naval Academy;
M.S., Industrial College of the Armed Forces, National Defense University.

Norman H. Crane
Systems and Technology Department;
B.A., Marietta College;
M.S., The Naval Postgraduate School.

Theresa A. Day
Defense Information Systems Agency Visiting Faculty, Information Strategies Department;
B.A., Western Illinois University;
M.B.A., St. Ambrose University;
D.B.A., Nova Southeastern University;
Harvard Senior Executive Fellow.

Michael J. Donohoe
Systems and Technology Department;
B.S., M.A., California University of Pennsylvania;
EMBA, University of Pittsburgh;
EMBA, Duquesne University;
D.Sc., Robert Morris University.

Cathryn Downes
Information Strategies Department;
B.A., University of Auckland, (New Zealand);
M.A., Ph.D., Lancaster University (United Kingdom).

Tammy Dreyer-Capo
Instructional Designer;
B.S. Idaho State University;
M.S. Towson University.

Mark R. Duke
Cyber Integration and Information Operations Department;
B.A., Sam Houston State University;
M.S., George Mason University;
M.A., Webster University.

Adrienne L. Ferguson
Chief Financial Officer Academy;
B.A., Grambling State University;
M.B.A., American University.

Paul H. Flanagan
Systems and Technology Department;
A.A., Richard Bland College;
B.S., Virginia Commonwealth University;
M.A., University of Maryland.

Michael B. Fraser
Visiting Professor, Faculty Chair, Dept. of Energy Department of Systems and Technology;
A.B., Stanford University;
M.S., Oregon State University;
Executive MBA, George Mason University.

Joanne Green
Instructional Designer;
B.S. Bloomburg University of Pennsylvania;
M.S. Marywood University.

Dennis Hall
Systems and Technology Department;
B.S., University of Illinois;
M.S., University of Illinois;
M.S., George Washington University

Jay Holcomb,
Cyber Integration and Information Operations Department;
B.S., University of Maryland;
M.B.A., San Jose State University.

Carl (CJ) Horn, LTC, USA
Information Strategies Department;
B.S., United States Military Academy;
M.A., Ph.D., The Ohio State University.

John S. Hurley
Information Strategies Department;
B.S., Florida State University,
M.S., Florida State University,
Ph.D., Howard University.

Marwan M. Jamal
Cyber Integration and Information Operations Department;
B.S., M.S., Ph.D., The George Washington University.

James E. Kasprzak
Cyber Integration and Information Operations Department;
B.S., Canisius College;
U.S. Army Command and General Staff College;
Air War College;
Ph.D., Loyola University.

Con Kenny
Systems and Technology Department;
B.S., University of Pennsylvania;
M.S., George Mason University.

Daniel T. Kuehl
Cyber Integration and Information Operations Department;
B.A., Allegheny College;
M.A., Temple University;
Ph.D., Duke University.

Katrice N. Lewis
Cyber Integration and Information Operations Department;
B.S., Loyola College;
M.S., University of Michigan-Ann Arbor.

Samuel Liles
Cyber Integration and Information Operations Department;
B.S.C.S, Huron University;
M.S.C.S., Colorado Technical University.

Russell H. Mattern
Systems and Technology Department;
B.S., U.S. Air Force Academy;
M.S., Ohio State University;
M.S., Industrial College of the Armed Forces, National Defense University;
M.S., Troy State University;
O.D., Ohio State University.

H. Mark McGibbon
Lockheed Martin Visiting Faculty, Systems and Technology Department;
B.S., University of Utah;
M.S., Naval Postgraduate School;
Ph.D., Northcentral University.

Robert A. Miller
Cyber Integration and Information Operations Department;
B.A., University of Chicago;
Ph.D., Princeton University;
J.D., The George Washington University.

Edward M. (Matt) Newman
Systems and Technology Department;
B.S., University of Maryland;
M.S., The American University.

John O'Brien
Information Strategies Department;
B.A., Roosevelt University;
M.P.A., Governors State University;
M.S., Air Force Institute of Technology;

Kristy Pron
Instructional Designer
B.S., M.S., Drexel Univeristy

Peter G. Rodgers, LCDR, USN
Information Strategies Department;
B.S., United States Naval Academy;
M.A., Naval War College.

Daniel J. Ryan
Cyber Integration and Information Operations Department;
B.S., Tulane University;
M.A., University of Maryland;
M.B.A., California State University;
J.D., University of Maryland.

John H. Saunders
Cyber Integration and Information Operations Department;
B.S., The Pennsylvania State University;
M.B.A., Ph.D., The George Washington University.

Kathleen M. Schulin
Information Strategies Department;
B.A., George Mason University;
Industrial College of the Armed Forces, National Defense University;
M.P.A., D.P.D.S., University of Southern California.

Geoffery W. Seaver
Information Strategies Department;
B.S., University of Kansas;
M.P.A., San Diego State University;
M.S.S.M., University of Southern California;
M.A., Naval War College;
Ph.D., The George Washington University.

Stephen B. Sledge, LTC, USA
Information Strategies Department;
B.A., Virginia Polytechnic Institute and State University;
M.I.P.P., The Johns Hopkins University (SAIS);
M.S., University of South Florida.

Dwight V. Toavs
Information Strategies Department;
B.S., Montana State University;
Air Command and Staff College;
M.P.A., University of Oklahoma;
Ph.D., Virginia Polytechnic Institute and State University.

Veronica Wendt
Systems and Technology Department;
B.S., United States Military Academy;
M.S., University of Maryland University College.

Contact Information

http://www.ndu.edu/icollege

Telephone:

(Dial direct by using the prefixes followed by the four digit extension of the office you wish to reach.)

Commercial	(202) 685-xxxx
DSN	325-xxxx

Administration

Chancellor	3886
Dean of Students and Administration	3885
Dean of Faculty and Academic Programs	3884
Director, Advanced Management Program	2103
Office of Student Services	6300
Fax	4860
E-mail:	iCollegeOSS@ndu.edu

Department Chairs

Cyber Integration and Information Operations Department.	3889
Information Strategies Dept.	2020
Systems and Technology Dept.	2069
Chief Financial Officer Academy	4887
Faculty and Administrative Fax	3974

Mailing Address:

National Defense University iCollege
ATTN: Name or Duty Title
Building 62
300 5th Avenue
Fort McNair, Washington, D.C. 20319-5066

As a follow-up to the very successful cyber events in Singapore (July 2010), London (Oct. 2010), and Dubai (Feb. 2011), the NDU iCollege is continuing to host international events to develop and strengthen human and intellectual capital in the cyber arena. The college will engage high-level government, academic, and private sector speakers to provide critical cyber information in these key areas: preventing and combating cyber terrorism, establishing cyber policy, ensuring information security, defining cyber warfare, utilizing cloud computing, developing multilateral cyber initiatives, and more…. Conference organizers will work with U.S. Combatant Commands (COCOMs), local embassies, regional Ministries of Defense, and global best practice corporations to ensure various points of view/projects/lessons learned are all represented.

Perspectives from: Local and Global Governments, Regional and U. S. Military, and Global Best Practice Corporations.

SCHEDULED EVENTS:

- 27-28 September 2011 (Bangkok, Thailand)
- 21-22 February 2012 (Abu Dhabi, UAE)
- Summer 2012 (Singapore)
- October 2012 (NATO/Brussels)

For more information and registraton

www.ndu.edu/icollege

av1-9-14-11

Hosted by: U.S. National Defense University ***i*College** and International Student Management Office

Conference Point of Contact: **CoopersmithP@ndu.edu**
Alumni Point of Contact: **ThackerS@ndu.edu**

NDU iCollege - 300 5th Avenue, Marshall Hall, Fort Lesley J. McNair, Washington, DC 20319

NDU iCollege
National Defense University
300 5th Ave, Building 62
Fort McNair, Washington DC
20319
202.685.6300

www.ndu.edu/icollege

National Defense University