Information Resources Management College

National Defense University

Educate Inform Connect

2016-2017

Catalog

Table of **Contents**

Contents

Every effort has been made to ensure this NDU IRMC Catalog and Student Handbook is accurate. However, all policies, procedures, and academic schedules are subject to change at any time and without prior notification by the IRMC Chancellor or the University administration. The NDU IRMC reserves the right to publish and revise an electronic version of the Handbook. This updated version is posted on the iCollege website at: http://www.icollege.ndu.edu. The online version will take precedence over the printed copy. The Handbook published for the current academic year supersedes all previous versions. Any corrections or suggestions for improvement of the IRMC Student Handbook should be directly communicated to the Office of the Dean at iCollegedean@ndu.edu.

MESSAGE FROM THE CHANCELLOR

As we look forward to Academic Year 2016-2017, your Information Resources Management College (iCollege) is excited to continue the development of our cyberspace education programs to meet the current and future needs of the Department of Defense and our many partners in the interagency, across the whole of government, in the private sector and internationally.

Last year I reported that the iCollege was transforming to include educational programs addressing the needs of leaders and advisors who conduct military operations in cyberspace in addition to those who leverage and design and develop, invest in, manage, and operate our information systems and technologies. The evidence of our successful efforts to do so is clear.

On 9 June 2016, the iCollege awarded 91 Master of Science in Government Information Leadership degrees to highly deserving graduates. I was proud to hand diplomas to these men and women who made the decision to gain the expertise in this domain that is so critical to our security. Included in the group that attended the graduation ceremonies was our first international master's degree graduate, Dragan Mladenovic from Serbia. I was so pleased that he traveled to join us for the occasion – truly a banner day for him, his nation, and for the iCollege.

Also among the graduates was the Department of Defense's first Senior Service College (SSC) class of students whose studies centered on employing information and cyberspace to achieve national security outcomes. The 14 military and civilian students spent ten months in a rigorous program of study focused on developing the habits of mind, conceptual foundations, and cognitive faculties needed to successfully employ information and cyberspace capabilities. The program included engagements with strategic practitioners, visits to critical cyberspace organizations, competing in the Atlantic Council Cyber 9/12 Competition, and an overseas practicum to EUCOM, AFRICOM, NATO, and Estonia during which they engaged with senior military leaders, civilian leadership of the alliance and with governmental officials who have lived through cyber attack. The military members of the class received their degree and will receive Joint Professional Military Education Level II credit for completing the program.

Of note, one of the SSC graduates, LTC Alan Dinerman, took advantage of his time at National Defense University (NDU) to collaborate with Dr. Jim Chen of the iCollege faculty to develop a paper and presentation titled, "On Cyber Dominance in Modern Warfare." As I write this, Dr. Chen and LTC Dinerman have been invited to present their work at the 15th European Conference on Cyber Warfare and Security to be held at the Bundeswehr University, Munich, Germany in July 2016. The iCollege is supporting their travel to the conference and I look forward to many future students making contributions to academic thought about cyberspace.

We marked the completion of another academic year with the of the presentation of the iCollege Hall of Fame Award to Ms. Melissa Hathaway for her constant support of the iCollege's objectives and her notable achievements in providing advice and counsel to senior governmental leaders and the private sector with

regard to cyber security. The award was presented in a combined ceremony in which we presented program diplomas for the Spring 2016 Chief Information Officer (CIO) Leadership Development Program (LDP) cohort that was just concluding its 14 week educational journey. During the year we also graduated a CIO LDP cohort in the fall. We're very proud of this innovative program which assembles a diverse pool of military, civilian, and international students to study leadership through the lens of the CIO competencies.

The CFO Academy continued to teach military and civilian leaders in the federal government's financial management cadre. The academy taught on site courses, presented at financial management conferences, worked with the Office of Management and Budget (OMB) at OMB sponsored CXO workshops, and provided on the spot education at DoD sponsored events to meet financial management certification requirements, and at civilian agency workshops addressing Federal financial management and strategic leadership lessons. International collaboration continued to be of high importance to the college. Various meetings and engagements allowed us to exchange ideas, offer assistance and support partnerships with countries including Germany, Sweden, Brazil, Vietnam, Israel, the United Kingdom, Australia, Denmark and Mexico. Participants were government, military and private sector representatives. Many sessions were focused on advice and counsel for these nations to develop their own cyberspace educational initiatives.

You should be aware that I have placed sustainment of program quality and curricular relevance at the top of my academic priority list. This has generated some key changes. First, the iCollege is adopting a more normal academic year schedule to include two semesters and a short summer break. We are doing this to provide faculty and staff with better planning horizons to coordinate curriculum changes, facilities improvements, and team initiatives, and to simply provide an opportunity for faculty and staff to catch their breath and prepare for the coming academic year. We are also reducing the per faculty teaching hours to provide the time and space for faculty to more intently engage in keeping their curricula fresh and current and to engage in research to enhance their curricula and to provide thought leadership in the cyberspace domain. This does mean that course offerings will be somewhat reduced, and that does impact you. Nonetheless, it is important to ensure that you receive the standard of quality in your education that is needed. The re-baselining of faculty classroom hours will not disrupt our efforts to provide education in context at sites other than NDU. Teaching at COCOMs and off-site locations is a way we can make our education more readily available to students who need it and we will continue to do so. The implementation of a more stringent application process will ensure that all students will be able to achieve that standard.

On a more practical note, efforts are well underway to renovate and upgrade many of our classrooms. The disruption will be very well worth it. Newly renovated rooms will give us the kind of connectivity and technology support needed for our programs and to support enhanced student collaboration. We expect to occupy the new rooms sometime late in the fall term.

In summary, your iCollege is doing very well. Our faculty and staff have demonstrated their commitment to student and stakeholder success. Watch for us to be more involved in cyberspace thought leadership through research, conference hosting, international engagement and alumni outreach. We are working hard to serve you and our stakeholders as we transform cyberspace education.

RADM (Ret) Jan Hamby, USN
Chancellor, NDU iCollege

Mission

The NDU Information Resources Management College (NDU iCollege) educates and prepares selected military and civilian leaders and advisors to develop and implement cyberspace strategies, and to leverage information and technology to advance national and global security.

The iCollege **Overview**

The Information Resources Management College (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. Whether in pursuit of the Master of Science in Government Information Leadership, a NDU iCollege Certificate, or a graduate level course for professional development— iCollege students bring diverse perspectives to 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.

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.

Academic **Departments**

The following academic departments conduct the College's educational programs:

Chief Financial Officer (CFO) Academy & Chief Information Officer (CIO)

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 Master of Science (M.S.) Degree Program.

The CIO Department focuses on the strategic-level concepts and practices necessary for successfully managing an organization's information resources. This perspective, based on the Clinger-Cohen Act (CCA) of 1996, includes delivering courses which address policy, planning and budgeting, performance measurement, process improvement, and portfolio management. Together, these and other courses form the iCollege's CIO Certificate Program. The department works closely with other departments to prepare iCollege graduates for leadership positions in the offices of CIOs across DOD and the Federal Government. In addition to the CIO Certificate, the CIO Department also delivers its concentration in the M.S. Degree Program.

Information, Communications, & Technology

The ICT Department sponsors the IT Program Management (ITPM) certificate and its concentration in the Master of Science (M.S.) degree program. The department also offers courses to support students completing the discontinued Enterprise Architecture (EA) Certificate and M.S. degree concentration. ICT courses focus on developing students for 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. Additionally, ICT courses examine IT program management, acquisition, enterprise architecture strategies, business case development, and data management strategies.

Cyber Security Studies

The CS Department focuses on government strategic leadership as it relates to information assurance, cyber security, and the role of information operations and cyberspace operations in the planning and execution of national and military strategies. The Cybersecurity (Cyber-S) Chief Information Security Officer Certificate Program and Cybersecurity M.S. concentration consist of courses that emphasize cybersecurity issues and fundamental approaches to the protection of the nation's information infrastructure.

Cyber Leadership & Joint Education

The CLJ Department focuses on developing the skills and the desired leadership attributes necessary to be an effective strategic leader in the Cyberspace Domain. The Department does this through the Cyber-Leadership Certificate Program which focuses on the strategic leadership attributes and knowledge necessary to integrate and conduct cyberspace operations to achieve national security objectives. The Department also provides focused instruction on the use of cyberspace information in the planning and execution of national security policies, military strategy, and joint operations as a component of the Joint Professional Military Education (JPME II) taught by the National Defense University.

Active Student-Centered Learning Through **Technology**

All iCollege instructional facilities are equipped with audio/visual components to deliver resident courses. Our distance learning courses use a variety of online resources to include the Blackboard course management system, Google Apps for Education, web conferencing and various communication and collaboration tools. Other web based tools may be used depending on the course. The iCollege faculty frequently experiment with web based instructional tools to enhance the online learning experience.

BYOD - Bring Your Own Device:

NDU provides a campus-wide wireless network for student use. All students attending a residential class at the iCollege must bring their own device to class and will be required to sign a user agreement in order to access the academic wireless network. Students are strongly advised against bringing government furnished equipment (GFE) due to recurring incompatibility issues with GFE on the wireless network. More information about the policy can be found at the NDU iCollege website at icollege.ndu.edu

Cybersecurity – Experiential Learning Attack & Defend/SCADA:

IRMC operates cybersecurity experiential learning facilities to give students a hands-on exposure to addressing threats to information systems. The Cyber Attack/Defend Lab provides an environment to examine computer and network defense through exercises in intrusion techniques, mitigation, and forensics. The Supervisory Control and Data Acquisition (SCADA) Lab realistically simulates exploits of and protections for various industrial control system components, such as used in the electrical, oil, gas, water, and transportation industries.

Course Delivery **Formats**

NDU iCollege courses are offered to domestic and international students through our blended (eResident) model, distributed learning (DL), seminars for our Senior Service College cohort, as well as the CIO Leadership Development Program. See the NDU iCollege Schedule of courses for beginning and ending dates of courses. The Blackboard Course Management System (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 active 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.

eResident

The eResident format is a five week course that 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.

Week One - Online

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 starts in the second week. Students begin by signing in to Blackboard (Bb), retrieving their readings, assignments, and other course instructions. During this week of virtual engagement, students must complete the assigned readings, participate online, and complete the assignments.

The faculty leading the course section will assign a grade of "W" (Withdrawal) to students who do not sign into Blackboard and satisfactorily engage in the required activities (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.

All students must meet week one requirements whether taking a course for credit or for professional development.

Week Two - In Residence

During this fulltime 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.

Week Three - Online

The third week of the course is designed to synthesize learning and prepare students for the follow-on graded final assessment. Participation in synthesis is required and graded for students seeking credit for the course.

Weeks Four & Five - Online

The final two weeks of a course are dedicated to completing the final 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 section in the schedule).

Distributed Learning

The Distributed Learning (DL) format engages students and faculty virtually over 12 weeks via Blackboard. The first 10 weeks of course, students are engaged in online seminar. The final two weeks is dedicated for assessment completion. The end-of-course assessment is typically 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. Final assessments are due no later than the Monday following the 12th week.

Other Formats

Elective courses are offered for students in residence at Fort McNair attending National War College, Eisenhower School, and the College of International Security Affairs.

Seminars, symposia, workshops, and other educational activities are conducted by faculty to meet particular learning needs of organizations on specific issues and topics. For event inquiries, contact Patricia Coopersmith, Director of Outreach & Partnerships, at coopersmithp@ndu.edu, 202-685-2117.

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.

Objectives 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, ethical, 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
- Communicate at the strategic level demonstrating command of the topic, logical organization, compelling argument, and excellence in English grammar and syntax.

Curriculum and Degree Concentrations

The 36 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 the concentration area, 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), Cyber Leadership (Cyber-L), Cybersecurity (Cyber-S), and Information Technology Program Management (ITPM).

Subject to graduation time limit requirements, a student may only use up to eight eligible NDU iCollege courses completed prior to MS program admission (i.e. while in certificate-seeking status) toward attaining the MS degree. No courses from other institutions are accepted for transfer. Courses taken for non-credit/professional development are not eligible. All coursework applied toward a M.S. degree must be completed within seven years of the award of the degree. Course which exceed the seven-year time limit are invalidated and subject to repeat. Students will have a maximum of seven years from their date of acceptance to successfully complete the M.S. degree program. See admissions section of catalog or the iCollege website (https://icollege.ndu.edu) for more information. Current and prospective MS students should refer to policies section of the handbook for specific Master of Science admission and academic policies and procedures.

Capstone Course

Only admitted Master of Science students are eligible to enroll in and complete the 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.

Senior Service College/Joint Professional Military Education (JPME II) Pilot Program

The NDU iCollege provides a Senior Service College (SSC)/JPME Phase II curriculum that provides a graduate education focused on the information/cyberspace instrument of national power. Graduates of the program will be national security leaders and advisors who lead, develop, and apply the policies, strategies, and doctrine to successfully leverage information and cyberspace operations within the broader national security framework.

Students in the JPME II program earn a Master of Science in Government Information Leadership with a concentration in Cyberspace Strategy.

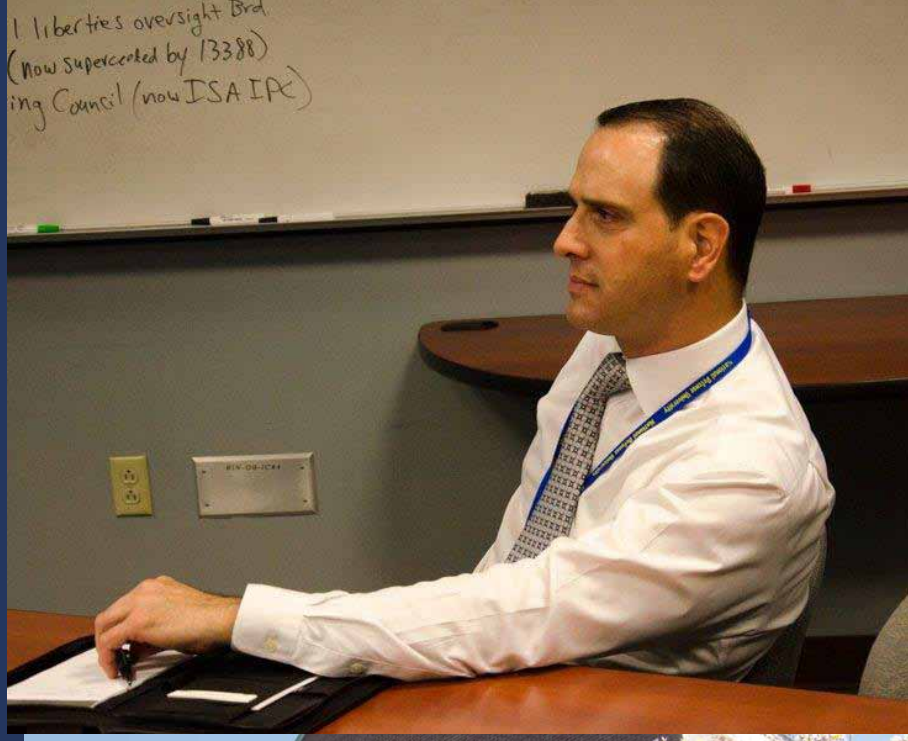
Students in the Cyberspace Strategy Program will be able to:

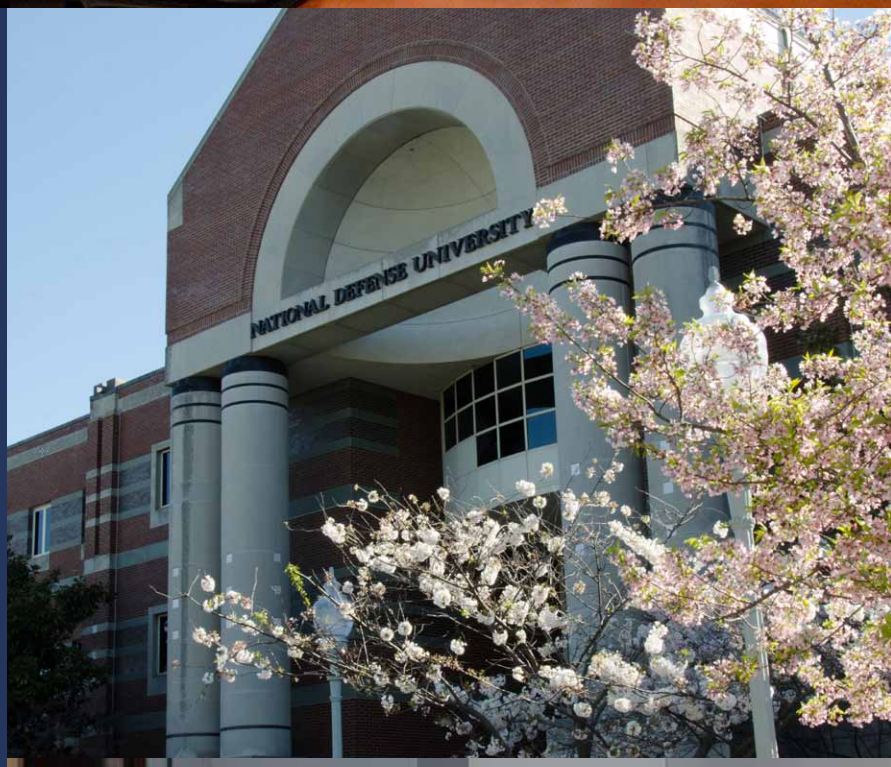
- Evaluate the national security environment with an emphasis on the use of the Information component of national power to achieve the Nation's strategic objectives
- Apply Joint Doctrine and JIIM perspectives to leverage information/cyberspace elements at the strategic and operational levels
- Understand the human-made terrain that underpins information and cyberspace operations and the resource management life cycle that supports that supports that terrain
- Demonstrate an expertise in strategic leadership, creative and critical thinking, decision-making, and a commitment to ethical conduct

Student Criteria:

Students for the NDU iCollege SSC pilot are nominated by their service or agency. Self -nomination or applications are not accepted. SSC nominees must be in the grade of O-5 and O-6 who have already received credit for completing a CJCS-accredited program of JPME Phase I or received equivalent JPME Phase 1 credit as articulated in CJCSI 1800.01E. Civilian students are equivalent to GS-14 and SES-1. The desired mix of seminar students includes military officers from all three Military Departments, the U.S. Coast Guard, international officers, DoD civilians, Federal Agency civilians, and the private sector. The curriculum is designed for students who currently serve in, have an interest in, or may have the need to develop strategy with those who serve in the information/cyberspace domain. A successful student does not need technical expertise, but must possess the intellectual curiosity that makes them receptive to new ideas and new approaches to understanding national security.

Certificates and M.S. Degree Concentrations





Chief Financial Officer (CFO) Leadership

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. All CFO Academy programs support and comply with DoD Comptroller's Financial Management Competencies.

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 financial professionals. The program highlights the changing role of CFOs as organizational leaders of 21st century government.

Successful CFO graduates will be able to:

- Lead within and across organizational boundaries by leveraging financial resources, information, technology, human resources, for strategic advantage;
- Achieve the goals of the Department of Defense financial management certification by evaluating the development and implementation of financial management strategies, policies, processes, operations and systems;
- Lead in an ethical manner at the enterprise level by linking critical decisions regarding resources, people, processes, and technologies to mission performance, decision support, information assurance, financial reporting, and financial systems security requirements;
- Synthesize theory and best practices from government, private sector, and not-for-profits to achieve organization's missions, and
- Communicate at the strategic level demonstrating command of the topic, logical organization, compelling argument, and excellence in English grammar and syntax.

CFO Leadership Certificate
6 Courses Required

Core (4)	BCP (6606)	White House, Congress, and the Budget
	CFF (6601)	Changing World of the CFO
	FFR (6607)	The Future of Federal Financial Information Sharing
	RIA (6608)	Risk Management, Internal Controls and Auditing for Leaders
Electives (2)		**Choose two Courses from Pool A or Choose one Course from Pool A and one Course from Pool B**
Pool A	AII (6203)	Information Assurance and Critical Infrastructure Protection
	ARC(6412)	Enterprise Architecture for Leaders
	COO (6504)	Continuity of Operations
	DMG (6323)	Decision Making for Government Leaders
	IPL (6411)	Information Technology Program Leadership
	ITP (6416)	Information Technology Project Management
	LDC (6301)	Leadership for the Information Age
	MAC (6512)	Multi-Agency Information-Enabled Collaboration
	OCL (6321)	Organizational Culture for Strategic Leaders
	PFM (6315)	Capital Planning and Portfolio Management
	PRI (6333)	Strategies for Process Improvement
	SPB (6328)	Strategic Performance and Budget Management (Previously MOP)
Pool B	DMS (6414)	Data Management Strategies and Technologies
	SEC (6201)	Cyber Security for Information Leaders
	WGV (6435)	Web-Enabled Government

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

Foundational (3)	CYS (6326)	Cyberspace Strategies
	OCL (6321)	Organizational Culture for Strategic Leaders
	CAP (6700)	Capstone Course
Core (4)	BCP (6606)	White House, Congress, and the Budget
	CFF (6601)	Changing World of the CFO
	FFR (6607)	The Future of Federal Financial Information Sharing
	RIA (6608)	Risk Management, Internal Controls and Auditing for Leaders
Leadership (2)	AII (6203)	Information Assurance and Critical Infrastructure Protection
	ARC (6412)	Enterprise Architecture for Leaders
	DMG (6323)	Decision Making for Government Leaders
	IPL (6411)	Information Technology Program Leadership
	LDC (6301)	Leadership for the Information Age
	MAC (6512)	Multi-Agency Information-Enabled Collaboration
Management (2)	COO (6504)	Continuity of Operations
	ITP (6416)	Information Technology Project Management
	PFM (6315)	Capital Planning and Portfolio Management
	PRI (6333)	Strategies for Process Improvement
	SPB (6328)	Strategic Performance and Budget Management (Previously MOP)
Technology (1)	DMS (6414)	Data Management Strategies and Technologies
	SEC (6201)	Cyber Security for Information Leaders
	WGV (6435)	Web-Enabled Government

Chief Information Officer (CIO)

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:

- Leverage CIO policy and organization competencies to lead within and across federal organizational boundaries by linking critical decisions regarding resources, people, processes, and technologies to mission performance.
- 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.
- Demonstrate abilities to construct and implement mission-aligned information and communication technology strategies [including gathering, analyzing, and reporting data; making decisions; implementing decisions; and evaluating organizational performance] in an ethical manner.
- Communicate at the strategic level demonstrating command of the topic, logical organization, compelling argument, and excellence in English grammar and syntax.

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 subject areas directly related to CIO competencies identified by the Federal CIO Council. 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 are based on each CIO competency. Students work with their supervisors and the iCollege'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 six (6) courses:

Three required core courses, and:

- One course from three different Security courses
- One course from four different Technology courses
- One course from six different Leadership/Management courses

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 for additional information.

CIO Leadership Development **Program**

Leadership Development Program

The Chief Information Officer Leadership Development Program (CIO LDP, or LDP for short) is the iCollege's flagship resident program for rising senior-level managers and leaders responsible for promoting and attaining national and international security goals through the strategic use of information and information technology as identified in the CIO competencies. The CIO LDP is administered in an intensive and highly interactive fourteen week forum. The student-centered educational experience emphasizes developing leadership skills and abilities while learning CIO content through completion of six courses. The leadership skills and abilities are put into practice and the learned knowledge is employed as students participate in a domestic field study. The domestic field study examines how private and public sector organizations implement CIO competencies. CIO LDP students form a learning community that fosters multiple perspectives on a wide range of issues.

The CIO LDP curriculum provides participants with the Chief Information Officer certificate and the CIO-LDP diploma as well as course work applicable toward the Master of Science in Government Information Leadership (CIO Concentration).

Spring Cohort

January 25, 2017 – April 28, 2017

Fall Cohort

August 9, 2017 – November 17, 2017

CIO LDP Application Instructions

Refer to the Admission Policies section for program eligibility and application instructions, and the Student Services Section for fees and payment instructions.

CIO Certificate
6 Courses Required

Core (3)	CIO (6303)	CIO 2.0 Roles and Responsibilities
	ITA (6415)	Strategic Information Technology Acquisition
	SPB (6328)	Strategic Performance and Budget Management (Previously MOP)
Security (1)	AII (6203)	Information Assurance and Critical Infrastructure Protection
	ESS (6206)	Enterprise Information Security and Risk Management
	SEC (6201)	Cyber Security for Information Leaders
Technology (1)	GEN(6206)	Global Enterprise Networking and Telecommunications
	DMS (6414)	Data Management Strategies and Technologies: A Managerial Perspective
	EIT (6442)	Emerging Information Technologies
	WGV (6435)	Web-Enabled Government: Facilitating Collaboration and Transparency
Leadership/ Management (1)	ARC (6412)	Enterprise Architectures for Leaders
	DMG (6323)	Decision Making for Government Leaders
	IPL (6411)	Information Technology Program Leadership
	ITP (6416)	Information Technology Project Management
	LDC (6301)	Leadership for the Information Age
	PFM (6315)	Capital Planning and Portfolio Management

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

Foundational (3)	CYS (6326)	Cyberspace Strategies
	OCL (6321)	Organizational Culture for Strategic Leaders
	CAP (6700)	Capstone Course
Core (4)	CIO (6303)	CIO2.0 Roles and Responsibilities
	ITA (6415)	Strategic Information Technology Acquisition
	PFM (6315)	Capital Planning and Portfolio Management
	SPB (6328)	Strategic Performance and Budget Management
Leadership/ Management (3)	ARC (6412)	Enterprise Architectures for Leaders
	DMG (6323)	Decision Making for Government Leaders
	IPL (6411)	Information Technology Program Leadership
	ITP (6416)	Information Technology Project Management
	LDC (6301)	Leadership for the Information Age
	MAC (6512)	Multi-Agency Information-Enabled Collaboration
	PRI (6333)	Strategies for Process Improvement
Technology (1)	DMS (6414)	Data Management Strategies and Technologies: A Managerial Perspective
	EIT (6442)	Emerging Information Technologies
	GEN (6205)	Global Enterprise Networking and Telecommunications
	WGV (6435)	Web-Enabled Government: Facilitating Collaboration and Transparency
Security (1)	AII (6203)	Information Assurance and Critical Infrastructure Protection
	COO (6504)	Continuity of Operations
	ESS (6206)	Enterprise Information Security and Risk Management
	SAC (6444)	Strategies for Assuring Cyber Supply Chain Security
	SEC (6201)	Cyber Security for Information Leaders
	TCC (6215)	Terrorism and Crime in Cyberspace

Cyber Leadership (Cyber-L)

The NDU iCollege Cyber Leadership (Cyber-L) program focuses on developing the skills and desired leadership attributes necessary to be an effective strategic leader in the cyberspace domain. The program achieves this through a rigorous curriculum that enhances the understanding of all aspects of cyberspace and how to best integrate cyberspace with the other elements of national power to achieve the nation's strategic objective.

Successful Cyber-L graduates will be able to:

- Employ critical, strategic, ethical, and innovative thinking to lead 21st Century organizations.
- Exercise strategic leadership and critical thinking in the development and use of cyberspace, information, and information technology as an instrument of national power.
- Understand the technology and processes that create and support the man-made terrain that underpins information and cyberspace operations.
- Facilitate collaboration and integration of cyberspace and information technology capabilities in a multi-stakeholder environment.
- Communicate at the strategic level demonstrating command of the topic, logical organization, compelling argument, and excellence in English grammar and syntax.

Cyber-L Certificate
6 Courses Required

Core (4)	CYI (6232)	Cyber Intelligence
	CYS (6326)	Cyberspace Strategies
	IPC (6228)	International Perspective on Cyberspace
	MAC (6512)	Multi-Agency Information-Enabled Collaboration
Electives (2)	CBL (6204)	Cyberlaw
	CIP (6230)	Critical Infrastructure Protection
	DMG (6323)	Decision Making for Government Leaders
	EIT (6442)	Emerging Information Technologies
	LDC (6301)	Leadership for the Information Age
	SAC (6444)	Strategies for Assuring Cyber Supply Chain Security
	TCC (6215)	Terrorism and Crime in Cyberspace
	WGV (6435)	Web-Enabled Government: Facilitating Collaboration and Transparency

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

Foundational (3)	CYS (6326)	Cyberspace Strategies
	OCL (6321)	Organizational Culture for Strategic Leaders
	CAP (6700)	Capstone
Core (5)	CBL (6204)	Cyberlaw
	CYI (6232)	Cyber Intelligence
	IPC (6228)	International Perspective on Cyberspace
	MAC (6512)	Multi-Agency Information-Enabled Collaboration
-Choose One-	CIP (6230)	Critical Infrastructure Protection
	SAC (6444)	Strategies for Assuring Cyber Supply Chain Security
Leadership (2)	ARC (6412)	Enterprise Architectures for Leaders
	DMG (6323)	Decision Making for Government Leaders
	LDC (6301)	Leadership for the Information Age
Technology (1)	EIT (6442)	Emerging Information Technologies
	GEN (6205)	Global Enterprise Networking and Telecommunications
	SEC (6201)	Cyber Security for Information Leaders
	WGV (6435)	Web-Enabled Government: Facilitating Collaboration and Transparency
Management (1)	COO (6504)	Continuity of Operations
	PFM (6315)	Capital Planning and Portfolio Management
	TCC (6215)	Terrorism and Crime in Cyberspace

Cyber Security (Cyber-S)

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 respective staffs, and as cyber security managers. This program provides advanced education to respond to the requirements set forth in the Federal Information Security Management Act (FISMA).

The Cybersecurity (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.
- Communicate at the strategic level demonstrating command of the topic, logical organization, compelling argument, and excellence in English grammar and syntax.

Chief Information Security Officer (CISO) Certificate - 6 Courses

Core (4 Courses)

AII (6203)	Information Assurance and Critical Infrastructure Protection
ESS (6206)	Enterprise Information Security and Risk Management
SEC (6201)	Cyber Security for Information Leaders
ATO (6209)	Approval to Operate: Information System Certification and Accreditation

Electives (2 Courses)

CBL (6204)	Cyberlaw
CIP (6230)	Critical Information Infrastructure Protection
COO (6504)	Continuity of Operations
TCC (6215)	Terrorism and Crime in Cyberspace

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

Foundational (3)	CYS (6326)	Cyberspace Strategies
	OCL (6321)	Organizational Culture for Strategic Leaders
	CAP (6700)	Capstone
Core (5)	AII (6203)	Information Assurance and Critical Infrastructure Protection
	ATO (6209)	Approval to Operate: Information System Certification and Accreditation
	ESS (6206)	Enterprise Information Security and Risk Management
	SEC (6201)	Cyber Security for Information Leaders
- Choose One -	CBL (6204)	Cyberlaw
	CIP (6230)	Critical Infrastructure Protection
Leadership (1)	DMG (6323)	Decision Making for Government Leaders
	IPL (6411)	Information Technology Program Leadership
	LDC (6301)	Leadership for the Information Age
	MAC (6512)	Multi-Agency Information-Enabled Collaboration
Technology (2)	EIT (6442)	Emerging Information Technologies
	GEN (6205)	Global Enterprise Networking and Telecommunications
	WGV (6435)	Web-Enabled Government: Facilitating Collaboration and Transparency
Management (1)	COO (6504)	Continuity of Operations
	ITP (6416)	Information Technology Project Management
	IPC (6228)	International Perspective on Cyberspace
	TCC (6215)	Terrorism and Crime in Cyberspace

Information Technology Program Management (ITPM)

Information Technology Program Management (ITPM) is a Certificate and a concentration in the Government Information Leadership Master of Science Degree Program. The ITPM program is designed to meet the ever-increasing call for program managers across the federal government. The 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.

Successful ITPM graduates will be able to:

- Lead and manage complex IT acquisition and other projects and programs that create value for their organizations through enhanced mission performance.
- Apply higher order skills in critical thinking, negotiation, collaboration, and persuasion to synthesize solutions to program management challenges within and across organizational boundaries.
- Identify critical ethical issues facing IT project and program managers, evaluate them using both applicable standards of conduct and sound ethical reasoning, and implement ethical decisions consistent with the values of the project management discipline and government service.
- Evaluate the organizational value of new information technologies and develop strategies for employing them for strategic advantage.
- Communicate effectively using traditional and more innovative methods.

ITPM Certificate
6 Courses Required

Core (6)	EIT (6442)	Emerging Information Technologies
	IPL (6411)	Information Technology Program Leadership
	ITA (6415)	Strategic Information Technology Acquisition
	ITP (6416)	Information Technology Project Management
	PFM (6315)	Capital Planning and Portfolio Management
	SAC (6444)	Strategies for Assuring Cyber Supply Chain Security

Government Information Leadership (GIL) MS Degree
Information Technology Program Management (ITPM) Concentration
12 Courses Required

Foundational (3)	CYS (6326)	Cyberspace Strategies
	OCL (6321)	Organizational Culture for Strategic Leaders
	CAP (6700)	Capstone
Core (6)	EIT (6442)	Emerging Information Technologies
	IPL (6411)	Information Technology Program Leadership
	ITA (6415)	Strategic Information Technology Acquisition
	ITP (6416)	Information Technology Project Management
	PFM (6315)	Capital Planning and Portfolio Management
	SAC (6444)	Strategies for Assuring Cyber Supply Chain Security
Leadership (1)	ARC (6412)	Enterprise Architectures for Leaders
	DMG (6323)	Decision Making for Government Leaders
	LDC (6301)	Leadership for the Information Age
	MAC (6512)	Multi-Agency Information-Enabled Collaboration
Technology (1)	DMS (6414)	Data Management Strategies and Technologies: A Managerial Perspective
	GEN (6205)	Global Enterprise Networking and Telecommunications
	SEC (6201)	Cyber Security for Information Leaders
	WGV (6435)	Web-Enabled Government: Facilitating Collaboration and Transparency
Management (1)	COO (6504)	Continuity of Operations
	ESS (6206)	Enterprise Information Security and Risk Management
	PRI (6333)	Strategies for Process Improvement
	SPB (6328)	Strategic Performance and Budget Management
	TCC (6215)	Terrorism and Crime in Cyberspace

Course **Descriptions**

AII

Information Assurance and Critical Infrastructure Protection (6203)

This course provides a comprehensive overview of Information Assurance and Critical 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.

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.

ASA

Analytics and Simulation for Enterprise Architecture (6436)

Prerequisite: 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.

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.

BCP

White House, Congress, and the Budget (6606)

CFO Program students only

This course presents a strategic understanding of Federal budgeting and appropriations, with particular attention to the role of the White House and the 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.

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. The NDU iCollege department responsible for each Master of Science concentration will define the specific nature and detailed requirements for the type

of project suitable for the respective concentration, and decide how a particular project type is assigned to a specific student.

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, nonrepudiation, 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.

CFF

Changing World of the CFO (6601)

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.

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.

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.

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.

CYI

Cyber Intelligence (6232)

This course examines the cyber leader's role in cyberspace intelligence. As decision makers, cyber leaders both enable and consume intelligence related to cyberspace: as enablers, they formulate and implement intelligence policy and strategy, acquire and deliver enterprise level information technology ("strategic IT") systems, and plan, program, budget for, and execute intelligence programs in cyberspace; as consumers, they plan and execute intelligence activities in cyberspace or make decisions based on threats emanating in or through cyberspace. This course includes perspectives and issues applicable to the U.S. Intelligence Community (IC) in general and elements unique to cyberspace. It is not intended to impart intelligence-specific skills and tradecraft to professional intelligence officers, and no prior experience in or knowledge of intelligence is required.

CYS

Cyberspace Strategies (6326)

This course examines the cyberspace strategies used by the United States, key nations, and non- state actors. Students examine relevant policies and constraints which will significantly impact strategies and achieving desired goals. Cyberspace risks, conflicts, and potential resolutions are proposed and discussed within this course. Students evaluate cyberspace leadership, operational features, strategic trends, and enforcement and dispute mechanisms. Students assess the cyberspace strategies employed by individual citizens, the federal government (such as commerce, defense, and intelligence), private industry, non-governmental organizations, transnational and international organizations, and organized crime. Students examine the consequences, repercussions, and likely outcomes of next-generation cyberspace strategies and how they could possibly address and shape issues within the continually evolving cyberspace domain.

DAC

Defense Enterprise Architecture (6409)

Prerequisite: ARC

This course presents examines Department of Defense (DoD) policy, direction; guidance related to Enterprise Architecture development and implementation; and major DoD enterprise architectures direction such as the Joint Information Environment (JIE), Information Enterprise Architecture (IEA) and the Business Enterprise Architecture (BEA).

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.

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, enterprisewide, 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.

DRR

Directed Readings and Research (6691/6692/6693)

Variable credit (1-3 credits) independent readings and research related to a topic of special interest to the student. Written assessment required.

EIT

Emerging Information 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 will be introduced to an array of emerging information technologies at various levels of maturity. Students analyze how emerging information technologies evolve. They evaluate the international, political, social, economic and cultural impacts of emerging information technologies using qualitative and quantitative evaluation methods. Students assess emerging information technologies using forecasting methodologies such as monitoring and expert opinion, examining future trends, and assessing international perspectives.

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.

FFR

The Future of Federal Financial Information Sharing (6607)

CFO Program 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.

GEN

Global Enterprise Networking and Telecommunications (6205)

This course focuses on the effective management of network and telecommunication 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 operations. Topics covered include JIE, the role of cybersecurity risk in networks and technology deployment, joint spectrum management, data visualization for network security, DevOps and cloud migration, mobile computing and network policy / governance to promote innovation

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. Students explore the cyberspace policies and strategies of various countries and regions as well as the cultural factor that leads to various international perspectives on cyberspace. Students also learn how to anticipate and respond to surprise and uncertainty 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.

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.

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.

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.

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.

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.

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 the Common Approach to Federal EA (CAFEA), 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.

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.

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 simulation of an IT investment portfolio review by the Investment Review Board.

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).

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.

RIA

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

CFO Program 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.

SAC

Strategies for Assuring Cyber Supply Chain Security (6444)

This course explores the strategies necessary to manage global supply chain risk within the Department of Defense and across the federal government. Students examine how cyber leaders (i.e. CIO, CTO, and IT Program Managers) can secure the supply chain through an understanding of trusted mission systems, supply chain risks and the role of supply chain participants. Students address the challenge of assessing global supply chain risk and delivering reliable and secure technology to agency staff and the warfighter. They examine a range of disciplines including governance, intelligence analysis, legal and regulatory compliance, and software and information assurance.

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.

SIO

Strategic Information Operations (6214)

Top Secret/SCI Clearance Required
U.S. Citizens Only

The course explores the national security concept of "strategic fragility" as it applies to modern society's growing reliance on interconnected, complex, and potentially fragile critical infrastructures. The course covers the rise of fragile infrastructures, the role of the information infrastructure as a control mechanism, sources of vulnerability, examples of infrastructure attacks and their consequences, and potential means to mitigate risks and deter attacks by others on our strategic infrastructures. The course also examines current roles and missions of various U.S. Government entities and military commands in light of the potential threat from strategic infrastructure attacks.

SPB

Strategic Performance and Budget Management (6328)

This course is an executive level view of strategic planning, performance management, and performance budgeting in public sector organizations. Using the Government Performance and Results Act and Kaplan & Norton's Balanced Scorecard as frameworks, students examine the linkage of mission to strategic planning, performance management, measurement, operational strategies, initiatives, and budgets to support senior level decision making. Emphasis is on transparency, outcomes, and linkage between organizational performance and the organization's budget. With this critical understanding, students develop leadership strategies that shape fiscal budgets to achieve agency strategic outcomes.

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.

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.

Academic **Partners**

The NDU iCollege continues to maintain academic partnerships with regionally accredited universities whose degrees align well with the college's educational programs. Graduates from our many certificate programs can apply to a number of partner institutions for completion of a Master's or Doctoral/PhD Degree. There are a multitude of degree choices for NDU iCollege graduates at the partner institutions.

Academic partners generally accept 9 or 12 graduate semester credits depending on which certificate program and how many courses were completed at the NDU iCollege. Students enrolled in iCollege programs prior to mid-2014 may receive up to 15 transfer credits, depending on which certificate was earned. For example, students graduating from the CIO Certificate with 8 courses will receive 15 transfer credits at selected partner schools, while those in the revised CIO program (6 courses) will receive 12 transfer credits.

Currently, there are more than 30 current NDU iCollege academic partners, which are listed below. Many partners provide full-time, part-time, and/or online educational opportunities. Several iCollege partner universities updated their agreements over the previous year to include new degrees and acceptance of additional NDU iCollege certificates. Please check our website often for changes and additions: http://icollege.ndu.edu/Academics/AcademicPartners.aspx .

Questions about the Academic Partner Program should be directed to the Director of Outreach & Partnerships, at 202-685-2080. Specific questions about degree programs, admission requirements, or remaining courses should be directed to the academic partner institution Point of Contact (POC) listed on the iCollege website.

Current NDU iCollege **Academic Partners**

Auburn University (AL)

California State University, San Bernardino (CA)

Capitol Technology University (MD)

Central Michigan University (MI)

East Carolina University (NC)

Florida Institute of Technology (FL)

Fort Hays State University (KS)

George Mason University (VA)

Global Information Assurance Certification (GIAC, a SANS Affiliate)

Illinois Institute of Technology (IL)

James Madison University (VA)

Johns Hopkins University (MD)

Missouri University of Science & Technology (MO)

New Jersey City University (NJ)

New Mexico Tech (NM)

Northeastern University (MA)

Nova Southeastern University (FL)

Pace University (NY)

Regis University (CO)

San Diego State University (CA)

Southern Methodist University (TX)

Syracuse University (NY)

University of Arkansas at Little Rock (AR)

University of Detroit Mercy (MI)

University of Illinois at Springfield (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 Texas at San Antonio (TX)

University of Tulsa (OK)

University of Washington (WA)

Walsh College (MI)

Alumni Career-Long Learning **Opportunities**

The National Defense University's Guiding Principles state that the University shall always foster and promote an environment that nurtures individual intellectual development and physical well-being and encourages career-long learning. IRMC mirrors this commitment to with our Alumni to enjoy lifelong learning beyond graduation.

Students who have graduated with an M.S. in Government Information Leadership are invited to return to IRMC to take additional courses for career-long learning, enrichment, and renewal of skills. These courses may be taken for credit or audited (see below). Alumni will be registered for courses on a space-available basis.

Students Electing Courses for Non-Credit

Alumni may also take a course for non-credit. Students must discuss their intent to take a course for non-credit with each Section Leader, and satisfy attendance and participation requirements for the course as outlined in its assessment plan. See the academic policies section for more information.

Admissions, Registration, and **Program Completion Policies**

Minimum Admission **Eligibility Criteria**

Education	All applicants must possess a Bachelor's degree from a regionally accredited U.S. institution or the equivalent from a foreign institution.
Grade/Rank Requirements for CIO, Cyber-S, Cyber-L, ITPM See page 9 for SSC/JPME requirements	Federal civil service pay grade of GS-13 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.
CFO Leadership Additional Requirements	Federal civil service pay grade of GS-14 or equivalent/military officer rank of 0-5 or above. (High performing GS-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. All applicants must provide a résumé 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.

Admission to Multiple Academic Programs

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

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:

SATFA Contact:

TRADOC SATFA (ATTG-TRI-SXX), Bldg. 950,
950 Jefferson Ave.,
Fort Eustis, Va.
23604-5724

In addition to the SATFA application process, students must submit an iCollege student application, available on the iCollege website.

International students must demonstrate comprehension 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 admission. 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 ECL 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.

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.

Pending Status

International Students will be placed in a Pending Status until Admissions Documents have been received and accepted. Students who do not provide required documentation prior to course completion cannot receive course graduate credit.

Application for **Admission**

Required Documents for Certificate and M.S. Degree (see next page for description):

- Application for Admission (Apply online at icollege.ndu.edu)
- Résumé
- 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.
- Writing Sample
- Nomination Letter (CIO-LDP Applicants Only)

To Apply:

U.S. applicants should submit all of the required documents in the same application packet. International applicants, please see previous section on international student enrollment for SATFA guidance.

Mail completed packets to:
NDU iCollege Office of Student Services
300 5th Avenue, Marshall Hall
Fort McNair, Washington, DC 20319

Admissions Calendar

Applications are reviewed twice a year for certificate and M.S. programs.

Admissions for Fall Term, 2017

January 15, 2017 – Application Period opens
March 1, 2017 – Complete Applications Due, including all supplemental materials
April 1, 2017 – Notifications of Admission Sent
April 15, 2017 – Registration for Fall 2017 opens

Admissions for Spring Term, 2018

See icollege.ndu.edu for spring term dates.

Admission Documents Descriptions

1. ### Application for Admission

   Application forms can be downloaded at https://icollege.ndu.edu

2. ### Résumé

   A résumé (maximum 3 pages) should include the last five years of work history that describes the applicant's position title, organization, responsibilities, and accomplishments. If there are gaps in the résumé, a short paragraph is needed to explain them.

3. ### Letters of Recommendation

   Recommendations should be completed on either the recommendation form provided on the NDU iCollege website, or on organizational letterhead. All recommendations, regardless of format, must address the questions asked on the form. For the M.S. program, at least one recommendation must come from a current or past supervisor. 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 can be uploaded on the application site or mailed to the IRMC Office of Student Services.

4. ### 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 3.3 in 6 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.

5. ### Writing Sample

   You will be asked to submit a 500 word writing sample responding to the topic required on the application.

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).

Notification of Admission

Applications will be notified of admission by the Office of Student Services.

Course Registration

Students who are admitted to the NDU iCollege will be sent detailed instructions regarding course registration, account information for online systems, and advisor information. Course descriptions and section dates/formats are available on the college's website. Members of special program cohorts will receive registration instructions from the program director.

Confirmation of Course Registration

Students will receive a course status email (enrolled/waitlisted) within 7 to 10 business days of their course request. 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 for one or more eResident sections when instructional periods do not overlap (i.e., the instructional period in the first three weeks of a course). Students are typically not allowed to take more than one DL course per semester. Students may seek permission to register for two concurrent DL courses. However, students will not be registered in concurrent DL courses unless there is available space in the second course. The second course request will automatically be placed onto the waitlist. Fifteen days before the beginning of the DL session, students will be notified if space is available in the second session.

Permission to register for more than one concurrent (DL) course may be granted by requesting an exception to policy (maximum 2 courses per session). Requests will only be considered for students who have successfully completed a previous DL course. 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 by sending an email to the Office of Student Services (iCollegeOSS@ndu.edu).

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.)

Course Cancellation

Due to low enrollment or other unavoidable circumstances, sometimes course sections must be cancelled. Course sections will be cancelled prior to the beginning of the course. However, the courses may be cancelled just prior to the course start date. Notification will be made to the email address on file in the student information system. It is inadvisable to purchase non-refundable plane tickets prior to the course start date, if required.

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 sections and the Chief Information Officer Leadership Development Program, but may not include special sections such as executive or special seminars.

Fiscal Year 2016 - 2017 Tuition*		
Employer Category	Course	Chief Information Officer Leadership Development Program (CIO LDP)
DOD civilian, Active U.S. Military & Uniformed Services, Active Military Reserve or National Guard	None	None
Non-DOD civilian, State and Local government	$1100	$10750
Private Sector	$2200	$16900
*Fiscal Year 2016-2017: October 1, 2016 to September 30, 2017.		

Payment Instructions

Students should make all payments for courses no later than the first day of the section. If payment is not received, the account is considered delinquent and the student may not be admitted to the course. Future registrations will be revoked or disallowed until the account is made current.

The NDU iCollege cannot accept cash payments. Valid forms of payment are credit card, check, 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 prior to the course start date.

Program Completion

Master of Science (M.S.) Degree Program: All coursework applied toward a M.S. Degree must be completed within seven (7) years of program admission. Courses taken after the seven year deadline will be subject to repeat, although the credit itself will not be revoked. Additionally, students have seven years from the date of admission to successfully complete their M.S. degree.

Graduate Certificate Programs: All coursework applied toward a certificate must be completed within four (4) years of program admission. Courses taken after the four year deadline will be invalidated and subject to repeat. Additionally, students have four years from the date of admission to successfully complete their certificate.

Students must successfully complete at least one course every 12 months to maintain active status in NDU iCollege programs. Students not completing at least one class every twelve months will be administratively withdrawn. Students so withdrawn may reapply for admission. An approved leave of absence will stop the student's program completion timeline (see section General Policies- Leave of-Absence).

Graduation Diplomas and Certificates

Master's degree diplomas and program certificates are prepared annually for graduation exercises. Master's degree diplomas and 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.

Graduation Procedures

It is the student's responsibility to meet all program requirements and to apply for graduation as further described below. 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:

- Be admitted to and active in the academic program(s) he or she intends to complete.
- Complete all course requirements according to the program of study for their admitted program version year.
- Complete and submit the "Application for Graduation" form, found on the iCollege website. 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 email a 'program completion letter' signed by the Academic Dean to the student's email 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 may attend the National Defense University commencement ceremony held in early June of each year. Applications for graduation must be submitted to the iCollege Office of Student Services no later than 1 March.

The iCollege recognizes distinguished graduates with the following awards:

Distinguished Graduates Certificate and Master of Science

Distinguished Graduate (DG) Award recognizes the academic achievement of graduates of NDU iCollege Certificate and Master of Science programs. Students who consistently exceed standards with the grade of A or A- in all courses that fulfill program requirements are eligible for the DG award.

Chief Information Officer Leadership Development Program Distinguished Leader Award

The Chief Information Officer Leadership Development Program (CIO LDP) Distinguished Leader Award, sponsored by AFCEA, recognizes a member of the CIO LDP graduating class for outstanding academic performance, demonstrated leadership, and exemplary personal conduct. Candidates for the Distinguished Leader Award must earn an A or A- in each of their CIO LDP courses, and receive the majority of CIO LDP student and teaching faculty nominations based on their demonstrated leadership and exemplary personal conduct.

Sponsored Awards

Within each specific educational program, the iCollege recognizes and honors several graduate students that have shown academic achievement in their studies. These awards are sponsored by longstanding iCollege partner organizations. To receive an award, the graduate must be a DG in the Certificate earned.

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.

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.

Unofficial Transcripts

Students may request unofficial transcripts from the Office of Student Services. These requests will only be sent to the preferred email address on record.

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 type 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

Transcript Request Process

Students must request official 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/Academics/Registrar.aspx) 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
Washington, D.C. 20319-5066
Phone: (202) 685-2128 (DSN: 325)
Fax: (202) 685-3920 (DSN: 325)
University-Registrar@ndu.edu

General and Academic Policies

All students are responsible for knowing and understanding the academic policies of the university and their particular academic program, including deadlines, attendance, curriculum requirements, acceptable grades, and academic integrity.

Applying Coursework Earned Prior to Program Admission

Graduate Certificate Program Participants

The NDU iCollege does not accept transfer credits from outside institutions. iCollege courses taken for non-credit may not be used to fulfill certificate requirements. Eligible courses may be used to fulfill requirements across multiple certificate programs. All coursework applied toward a certificate must be completed within four years of program admission.

Master of Science Program Participants

Subject to the graduation time limit requirements, a student may use up to eight 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. NDU iCollege courses taken for non-credit may not be used to fulfill M.S. degree requirements. All coursework applied toward a M.S. degree must be completed within seven years of program admission.

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. Approval 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.

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 in all coursework attempted for academic credit.

Adminstrative Withdrawal

Students not completing at least one class every twelve months will be administratively withdrawn from the college. Students may reapply for admission.

Probation

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.

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 and/ or upon the decision of the Academic Review Board.

Reinstatement

Dismissed students who wish to request reinstatement must reapply for program admission. 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.

Academic Policies

Student Preparation

The iCollege recognizes its students bring a wealth of knowledge and experience with them. Accordingly, the College's courses are structured to obtain the maximum exchange of views among faculty and students. Classes are typically conducted in seminars, but occasionally include lecture, panel discussions, question-and-answer sessions with guest speakers, and student exercises. Key to this learning process is student preparation and active participation in classroom discussions and practical exercises.

Students are expected to prepare for each session by reading the material assigned for that lesson. Readings may be the focus for a seminar discussion or be a key part of an

in-class exercise or activity. In addition, readings provide a common knowledge base for additional information presented and discussed during the class. Faculty and seminar participants will assume that reading assignments have been completed by the start of the session.

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.

Course Credits

NDU iCollege eResident and DL courses are worth three (3) credit hours unless otherwise noted. JPME Electives courses offered through the NDU electives program are worth two (2) credit hours.

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.

C Grade: Only one grade of C may be used to fulfill certificate program requirements. The grade of C cannot be used to fulfill requirements for the Master of Science degree program. C grades may not be transferable 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; or a student is dismissed for violation of the NDU Academic Integrity Policy.

Grade Scale

GPA Grades (Credit Bearing Courses)		
Letter Grade	GPA Value	Description
A	4.0	Exceptional Quality
A-	3.7	Superior Quality
B+	3.3	High Quality
B	3.0	Expected/Acceptable Quality
B-	2.7	Below Acceptable Quality
C	2.0	Unsatisfactory
F	0.0	Fail/Unacceptable
Grades (Non-Credit Bearing Courses) For students enrolled in Professional Development Non-Credit courses, the grading is based on a Pass/Fail scale. The following Pass/Fail grades are approved for use in the determination of course performance.		
Letter Grade	Value	Description
P	0.0	Pass
F	0.0	Fail
Other/Non GPA Annotations/Actions (Academic Credit is Not Earned)		
I	Incomplete	
W	Withdrawal	

Non-GPA Annotations

Non-Credit Bearing Pass/Fail (P/F): The Pass/Fail grade is assigned to students who elect to take a course for non-credit. Pass (P) is awarded to students who successfully complete requirements except the final assessment. Students must retake courses for credit if they want to apply them to a program. Students will declare in writing if he/she is taking the course for non-credit by the Friday of the seminar week (week 2). DL students must declare by the Friday of the ninth DL week.

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 requirements for the course and request an extension in writing to the Section Leader prior to the assignment deadline. The written request should detail the unusual and extenuating circumstances that justify an extension and provide a proposed deadline for submission. Requests made to accommodate professional work related demands, with the exception of deployment, will not be granted. Students are expected to balance their academic and professional responsibilities.

The Section 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 Faculty and Academic Programs.

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).

Capstone Grade

The grade of B is the lowest possible passing grade for Capstone. Students may retake the Capstone only once. Students who are unsuccessful after their first Capstone attempt may be required to meet additional graduation requirements (e.g. Successful completion of an outside writing course).

Grade Submission

The faculty will assign a grade for each student in a course based upon the grading policy. The faculty will submit the course grades to the University Registrar via the appropriate electronic resource. A faculty member cannot change any student's grade after the course grade has been submitted. Any grade change request must provide documentation specifying the reason and have the approval of the Dean of Faculty and Academic Programs and the University Provost.

Grade Appeal Policy & Process

A student may challenge a final course grade if the student has a reasonable belief the grade was assigned in an arbitrary or capricious manner and is unable to resolve his or her concerns with the faculty member who assigned the grade. This policy applies only to final course grades and does not apply to course work or other grades awarded during course.

A student may only challenge a final course grade under this policy if the student has discussed the concern with the faculty member and can demonstrate that the grade was awarded in an arbitrary or capricious manner. For purposes of this policy, arbitrary or capricious means (a) the assignment of a final course grade was made on a basis other than the student's academic performance in the course (b) the assignment of a final course grade was made in a manner that substantially or unreasonably departed from the instructor's articulated standards.

This policy will not be used to review the judgment of an instructor in assessing the quality of a student's work, to require another faculty member to re-grade or re-examine a student's work, or in cases involving alleged violations of academic integrity.

1. If after discussion with the faculty member the student believes, in good faith, that the grade is arbitrary or capricious, or if there is an inability to reach the faculty member, the student may challenge the grade by sending a letter to the department chair no later than 30 calendar days after the grade has been posted. This letter must
   (a) identify the course, date, and faculty member that awarded the grade;
   (b) state the basis of the challenge, including all facts relevant to the challenge and the reasons the student believes the grade is arbitrary or capricious;
   (c) indicate the date(s) the student consulted with the faculty member regarding his or her concern(s) and summarize the outcome of those discussion(s); and
   (d) attach any supporting documentation the student believes should be considered in the challenge, including the syllabus.

2. Upon receiving a written challenge to a final course grade, the Department Chair shall forward a copy of the challenge to the faculty member who assigned the grade. The faculty member then has 15 calendar days from receipt of the challenge to provide a written response. The student will receive a copy of the faculty member's response; however, any information that would violate the privacy rights of other individuals will not be released to the student.

3. The Chair will review the submissions and, if necessary, investigate to determine if the grade was arbitrary or capricious based on the definition outlined in this policy. A written decision will be issued to both parties within 15 calendar days.

4. Both parties have a right to appeal the Chair's decision by filing a written appeal within 10 business days to the NDU iCollege of the Dean of Faculty and Academic Programs (The Dean). The written appeal should state the basis for the appeal and attach all relevant written documentation.

5. The Dean shall forward the appeal to the NDU iCollege Academic Policy Committee. The Academic Policy Committee will review the submissions and may, at the Committee's discretion decide to hear statements from the parties. Following deliberations, the Committee will issue a recommendation to the Dean (or designee) indicating:
   1. Whether the Committee finds the grade to be arbitrary or capricious and;
   2. The Committee's recommendations for the disposition of the appeal.

6. The Dean (or designee) will review the Committee recommendation and render a final decision in writing to the student, the faculty member, and the chair within 10 calendar days of receipt of the Committee's recommendation. The Dean's decision shall be final without further appeal.

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/Academics/AcademicPolicies.aspx 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; plagiarism, and breaking non-attribution policy.

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 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.

Non-Attribution Policy

Presentations by guest speakers, panelists, and renowned public officials and scholars constitute an important part of the curriculum. In order that these guests, as well as faculty and other officials, may speak candidly, the College offers its assurance that presentations will be held in strict confidence. This assurance derives from a policy of non-attribution that is morally binding on all who attend. Without the expressed permission of the speakers, nothing they say may be attributed to them directly or indirectly in the presence of anyone who was not authorized to attend the presentation. This policy is not intended to preclude references by students and faculty within the academic environment to opinions expressed by speakers; however, courtesy, good judgment, and the non-attribution policy preclude citing those views, even if the speaker is not identified by name, even when questioning subsequent guests. Specifically, the non-attribution policy provides that:

- Classified information gained during these presentations may be cited only in accordance with the rules applicable to its classification. Additionally, without consent, neither the speaker nor the College may be identified as the originator or source of the information.
- Unclassified information gained during lectures, briefings, and panels may be used freely within the academic environment; however, without consent, neither the speaker nor the College may be identified as the originator of the information.
- Breaking the non-attribution Policy is a breach of academic integrity.

Guest Speaker Procedures

Students are to be in their seats at least five minutes before the scheduled starting time, and will stand when the guest speaker(s) enters the room. As a courtesy, students will not enter late or leave the room before the conclusion of the question and answer session. It is customary to applaud the visiting speaker at the end of the introduction and to stand and applaud the visiting speaker at the end of the lecture and question and answer period.

Penetrating and thought-provoking questions are essential to a productive discussion session with the speaker. The iCollege expects students to be prepared and willing to ask good questions of the speaker. When asking questions, it is critical that the student identify him/herself and state his/her parent agency. This is a courtesy to help the speaker better answer the question. Speaker presentations and their associated question and answer session customarily are not recorded or transcribed and never without the expressed consent of the speaker. This policy is complementary to the non-attribution policy which encourages our speakers to discuss their subjects with candor.

Attendance Policy

Students are expected to participate in all scheduled class sessions and activities. The College will not issue course credit (or the grade of P for non-credit) if more than five percent of the class is missed.

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 may approve a maximum of two hours of missed class time. All absences exceeding two hours must be pre-approved by the Dean of Students.

NDU Code of Conduct

To advance the mission of educating, developing, and inspiring National Security Leaders, we must continually create and maintain an academic environment founded in a community of trust that demands excellence in professional conduct and ethical standards. Students must adhere to the highest standards of honor. Specifically, students will not lie, cheat, steal or otherwise behave in any way that discredits themselves or impugns on the reputation of their fellow students at National Defense University. Failure to follow these standards may result in administrative action, including dismissal from the University.

Dress Policy

Military and civilian personnel are expected to exemplify professional standards of dress and appearance. A business suit with tie or conservative sport coat with tie is considered appropriate dress for men; commensurate attire is expected of women. Military students may wear either the class B uniform or civilian attire as described above. Some events will require military students to wear the Dress Uniform.

Spouse Travel

NDU policy prohibits spouses and family members accompanying or meeting students and faculty members on field studies. This policy is strictly enforced and exists to eliminate any possible perceptions that field studies are not a full-time, professional endeavor.

Student Appeals

Student appeals are directed though the Office of the Dean of Faculty and Academic Programs for review and decision. Only written appeals with written documentation will be considered. Appeals should be submitted via e-mail to the iCollegeDean@ndu.edu.

Student Services and **Resources**

NDU iCollege Office of Student Services

The NDU iCollege Office of Student Services (OSS) is located in Room 145 Marshall Hall. Students should consult the OSS for assistance with admissions, registration, course management, tuition processing, and online student information system operations. Office hours are 0700-1500. The Office of Student Services can be reached by phone at (202) 685-6300 and by e-mail at iCollegeOSS@ndu.edu.

Disability Support

The Americans with Disabilities Act (ADA) provides civil rights protection for persons with disabilities. This legislation guarantees a learning environment that provides for reasonable accommodation for students with disabilities. If you believe you have a disability requiring an accommodation, please contact the NDU iCollege Office of Student Services - 202.685.6300 or iCollegeOSS@ndu.edu.

Directions to Fort McNair

Ft. McNair Campus Fort Lesley J. McNair
300 5th Avenue,
Washington, DC 20319

Which Gate to Enter**:** There are two post entry points: 1) The Main Gate (on P Street, at stoplight) for vehicles with a DoD decal, 2) the Visitor's Gate (at 2nd Street SW) for any vehicle. StudenDoD (military and civilian) or Government photo ID (state issued driver's license). DC area and facility badges (like NCR, MDW and your student badge) are not valid.

Post Security Inspection: Vehicles may be searched and are mandatory for some and random for all. If directed to report for a vehicle search, you must comply. All personal belongings brought into this post are subject to search.

Security

Students must show valid ID at the Marshall Hall Guard Desk upon entering Marshall Hall and wear ID badges in a visible place while participating in iCollege courses. The Guard Desk can be reached at (202) 685-3766. All personal property should be secured at all times. Do not leave purses or wallets in the classroom during breaks. Do not leave personal articles and clothing in the building overnight.

Class Hours

Classes start at 0800 and end by 1700 each day. Breaks are scheduled throughout the day. Students are expected to be prompt and prepared for all classes.

Transportation

The Washington, DC area has a number of public transportation options.
Information can be found at the following links:

- Washington Metro: http://www.wmata.com/
- Virginia Railway Express: http://www.vre.org/
- Maryland MARC Train: http://www.mtamaryland.com/services/marc/
- Amtrak Railway: http://www.amtrak.com/

Lost and Found

Report or turn in lost/found articles to the security guard on duty in the building where the article was lost/found. If theft of an item is suspected, first check to see if it has been turned in to the security guard. If not, notify the iCollege Office of Student Services, the NDU Security Office, and the Fort McNair military police (MPs). After the MPs complete their report, the case is turned over to Fort Myer for investigation. When the investigation is completed, a claim can be made against the government. Government claims require two estimates of loss with the Standard Form (SF) 95 when filing at the Fort Myer Claims Office (703) 696-0761. In general, the government will not pay a claim unless the property was secured at the time it was stolen.

Inclement Weather

When adverse weather conditions in the Washington, DC area necessitate closing federal offices, the University will also close. Students should call (202) 685-4700 from an off-campus phone to obtain guidance. Press option #2 at the voice menu. Alternately, students can check the OPM website at: http://www.opm.gov/status. In instances when the iCollege is closed or has a two-hour delay, students should check with their instructors via Blackboard or email to determine whether alternate course plans will be implemented.

NDU **Library**

The NDU Library is a world-class academic library with a full range of resources and services, and a staff dedicated to ensuring that all students achieve academic success. It is a 24/7 virtual library with branches in Washington, D.C. and Norfolk, VA. The Washington, D.C. Library is located in Marshall Hall.

Library Website – on campus: http://ndu.libguides.com/ndulib

Library Website – off campus: Use the "NDU Libraries" tab in Blackboard

MERLN: http://merln.ndu.edu

Hours: Monday-Thursday, 0700-1800; Friday 0700-1500

Location: 2nd and 3rd Floors Marshall Hall
Telephone: 202-685-3511
Email: library_reference@ndu.edu

Services

The Library is customer-oriented with high levels of service. Students all have access to ask-a-librarian, a virtual reference service that connects students to research assistance. Service to students emphasizes instruction on conducting independent research with the expert guidance of reference librarians, which allows students to explore the breadth of information on a topic and benefit from the discovery process. Librarians seek to instill information skills to develop effective search strategies, evaluate information sources critically, synthesize selected sources into personal knowledge, and use information effectively in scholarship. In addition, students have borrowing privileges to make use of the Library's extensive collections of print, audio-visual, and electronic resources. On-campus students have the opportunity to attend a library orientation program that introduces them to the wealth of resources. A variety of additional research classes can be taught online. Contact the Library to inquire about course offerings.

Collections

The Libraries house over 500,000 books, periodicals, and government documents. Subjects include national security strategy, cybersecurity, information and information technology, leadership, military history, homeland security, international affairs, warfare, foreign relations, military strategy and operations as well as many others. Blackboard accounts provide access to virtual collections including 100+ subscription databases covering an array of research topics, 20,000+ electronic journals, newspapers, dissertations, and magazines, and 125,000+ ebooks, many of them downloadable.

Special Collections

Archives and History. Located on the upper level of the library, Special Collections, Archives and History is the repository for personal papers, the NWC archives, student papers, lectures, rare books, local history, photographs, maps, prints and artifacts. The personal papers of twentieth-century military and diplomatic leaders, primarily those of former Chairmen and Vice-Chairmen, JCS, Supreme Allied Commanders, and other Combatant Commanders are collected. Papers of former Chairman, JCS, include those of Generals : Lyman L. Lemnitzer, Richard Myers, Peter Pace, Colin Powell, John Shalikashvili, Henry Shelton, Maxwell D. Taylor, John Vessey, and Admiral Mike Mullen. The SACEUR papers include those of Generals Andrew Goodpaster, Bernard Rogers, John Galvin, George Joulwan, Wesley Clark, and Admiral James Stavridis. Exhibits which support the curriculum and special events, as well as artwork, are organized by Special Collections. A resource for the history of Ft. McNair, the staff provides tours of the post and research support from the local history collections. Please call 685-3957/3969 for additional information.

Classified Documents Center (CDC)

The library's Classified Documents Center is located in Marshall Hall, Room 316. Proper clearance and positive identification are required to enter and use materials and services. Online networks (Intelink-TS and SIPRnet), secure meeting spaces, and storage boxes are available. Hours of operation are Monday-Thursday, 0730-1600; Friday, 0730-1500. Please call 685-3771 for more information.

MERLN

One-stop Web access provides timely information on military affairs, international relations, and security studies. MERLN contains the most comprehensive collection of Defense White Papers and national security strategies available on the Web with contributions from more than 85 countries. MERLN features the Military Policy Awareness Links (MiPALs), custom-made research guides created by the Library staff on topics such as Cybersecurity, National Security Strategy, Iraq, Iran, Afghanistan, and Terrorism. Each MiPAL offers U.S. policy statements supplemented by the latest collection of articles, reports, and analysis of U.S. policy options from a global network of think tanks. Additionally, MERLN hosts the U.S. National Strategy Documents, an in- depth collection that includes National Security Strategies dating from the Reagan Administration to the present day, Military and Defense Strategies, and Quadrennial Defense Review reports.

Campus **Facilities**

Food Service Operations

NDU's cafeteria is located in Lincoln Hall. The Lincoln Hall Café is open Monday through Friday, 0700-1430, in Room 1501 near the passenger elevators on the first floor. For more information call the cafeteria directly at (202) 685-7235.

The Fort McNair Officers' Club is located in building 60 on 2nd Avenue, three blocks west of the Marshall Hall front entrance. You can reach the Officer's Club at (202) 685-5800. The Officer's Club is open Monday - Friday.

Vending machines containing snacks and beverages are located in hallways near classrooms.

Fitness and Recreation Facilities

The main fitness center is located across from the NDU Lincoln Hall parking lot. Additionally, fitness centers are also located within the Roosevelt, Eisenhower Halls.

Medical Assistance

Routine medical care for military personnel are available on post at the Fort McNair Health Clinic, Building 58, from 0630-1500; call (202) 685-3100 for an appointment. Military sick call is on a walk-in basis from 0630-0830 and 1130-1300. Physicals, immunizations, and other services can be obtained by appointment.

U.S. Post Office

A branch office is located in Building 29 ((202) 523-2144), just inside the main gate. Hours of operation are 0815-1300 and 1400-1615 Monday through Friday. The facility is closed on Saturdays, Sundays, and recognized holidays.

Chapel

The Fort McNair Chapel, Building 45, is available for religious services, ceremonies, and programs. Call the Chaplain's Office at (202) 685-2856 for further information.

Shoppette/Gas Station

The Fort McNair Shoppette/Gas Station is open to everyone from 0800-1700, every day of the week and sells snack items, beer and wine, and gasoline. The phone number for the shoppette/gas station is (202) 484-5823.

State Department Federal Credit Union

Members of the State Department Federal Credit Union may conduct their banking at the Fort McNair branch in Building 41. The Credit Union can be reached at (703) 706-5127.

Barber/Beauty Shop

Fort McNair's Barbershop and the Beauty Salon are located in Building 41. Hours vary; for more information, call (202) 484-2354.

ATM

There is a State Department Federal Credit Union ATM located in the north end of Marshall Hall on the first floor.

Telephone Services

In cases of emergency only, incoming calls for students should be made to the Office of Student Services during regular business hours (0700-1500). The Office of Student Services can be reached at (202) 685-6300 or DSN 325-6300. Students will be contacted in their classrooms for emergency calls.

Dialing from University phones:

- To dial DSN, dial 94 then the DSN number.
- To dial a commercial number, dial 991 then the area code and number, as appropriate.
- To dial internally within NDU, please press 685 and then the extension (ex)685-xxxx

Faculty & **Administration**

LEADERSHIP

Jan Hamby RADM (Ret) USN
Chancellor
B.A. University of North Carolina Chapel Hill
M.S. Boston University
M.B.A. Boston University
M.A. U. S. Naval War College

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

Matthew Hergenroeder COL USA
Dean of Students
B.S. United States Military Academy
M.A. University of Redlands
M.S. Industrial College of the Armed Forces, National Defense University

Russell E. Quirici
Dean of Administration
Director - CIO LDP
B.S. United States Military Academy
M.A. The Pennsylvania State University
M.S. National War College, National Defense University

Cassandra C. Lewis
Associate Dean for Academic Programs
B.A. University at Buffalo
M.A. Boston College
Ph.D. University of Maryland, College Park

John T. Christian
Chair - Chief Information Officer Department & Chief Financial Officer Academy
B.A. University of Virginia
M.A. Ph.D. Vanderbilt University

James F. Churbuck
Chair - Cyber Security Department
B.S. United States Naval Academy
M.S. Industrial College of the Armed Forces, National Defense University

Carl (Cj) Horn
Chair - Cyber Leadership and Joint Education Department
B.S. United States Military Academy
M.A. Ph.D. The Ohio State University

Edward M. (Matt) Newman
Chair - Information, Communication, & Technology Department
B.S. University of Maryland, College Park
M.S. The American University

JoAnne Green
Director of Academic Computing
B.S. Bloomburg University of Pennsylvania
M.S. Marywood University

George Fulda
Director of the Office of Student Services and Institutional Research
B.A. Fairmont State University
M.A. West Virginia University
Ed.D. West Virginia University

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

FACULTY

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

Nancy Blacker COL USA
Army Service Chair
Cyber Leadership and Joint Education Department
B.A. University of Kentucky
M.P.A. Kentucky State University
J.D. University of Kentucky

Jim Chen
Cyber Security Department
B.A. M.A. Fudan University
Ph.D. University of Maryland, College Park
CERIAS Graduate Certification, Purdue University

Gregory Clay Lt Col USAF
Cyber Leadership and Joine Education Department
B. S. U.S. Merchant Marine Academy
M.B.A. University of Phoenix

Cathryn Downes
Cyber Leadership and Joint Education Department
B.A. University of Auckland (New Zealand)
M.A. Ph.D. Lancaster University (United Kingdom)

Michael Donohoe
Chief Information Officer Department
B.S., M.A. California University of Pennsylvania
EMBA University of Pittsburg
EMBA Duquesne University
D.Sc., Robert Morris University

Tammy Dreyer-Capo
Cyber Security Department
B.S. Idaho State University
M.S. Towson University

Mark R. Duke
Cyber Security Department
B.A. Sam Houston State University
M.S. George Mason University
M.A. Webster University

Roxanne Everetts
Cyber Security Department
B.A. The George Washington University
M.S. D.M. University of Maryland University College

Matthew Feehan
Cyber Security Department
B.A. Simpson College
M.S. National Intelligence University
Graduate Certificate: Chief Information Officer
National Defense University

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

Gerry Gingrich
Cyber Leadership and Joint Education Department
B.S. University of North Carolina
M.S. Ph.D. University of Maryland, College Park
Post-Doctoral Fellowship, University of Minnesota

Andrew P. Gravatt
Information, Communication, & Technology Department
B.S. University of Maryland
M.S. The Johns Hopkins University Whiting School of Engineering
M.S. IRM College, National Defense University

John Giuseppe CDR USN
Sea Service Chair
Cyber Leadership and Joint Education Department
B.S. The George Washington University
M.S. National War College

Dennis Hall
Information, Communication, & Technology Department
B.S. M.S. University of Illinois
M.S. The George Washington University

Stephen Hall LTC USA
Chief Information Officer Department
B.S. United States Military Academy
M.A. Teachers College, Columbia University

John S. Hurley
Information, Communication, & Technology Department
B.S. M.S. Florida State University
Ph.D. Howard University

Michael Jacobs
Information, Communication, & Technology Department
B.F.A The Savannah College of Art and Design

Marwan M. Jamal
Information, Communication, & Technology Department
B.S. M.S. Ph.D. The George Washington University

Michael Love LTC USA
Information, Communication and Technology Department
B.A. Duquesne University
M.S. Syracuse University

Stephen Lowe
Visiting Professor, Department of Agriculture Faculty Chair
Chief Information Officer Department
B.S. James Madison University
M.P.A. Virginia Tech
M.S.M.I.T. University of Virginia
Ph.D. University of Glasgow
Certificate of Cross Sector Leadership, Presidio Institute Fellows Program

Jennifer Mandula
Cyber Leadership and Joint Education Department
B.A. Davidson College
M.Sc. University of Oxford

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

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

Kenneth D. Rogers
Visiting Professor, State Department Faculty Chair
Chief Information Officer Department
B.A., Westmont College
M.P.I.A., University of Pittsburgh
M.I.M., University of Maryland
M.S., George Washington University
Graduate Certificates: Asian Studies and International Political Economy – University of Pittsburgh
Graduate Certificate: CTO Innovation & Emerging Technology – Stanford University

Dennis Ruth
Visiting Chair, Defense Information Systems Agency
Cyber Security Department
B.S. University of Illinois Chicago
M.S. Boston University
US Army Command and General Staff College

Julie Ryan
Cyber Security Department
B.S., U.S. Air Force Academy
M.L.S., Eastern Michigan University
D.Sc., George Washington University

Geoffery W. Seaver
Chief Information Officer 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

Paul Shapiro
Information, Communication and Technology Department
B.S. University at Buffalo
M.B.A. George Mason University
Ph.D. The George Washington University

James Skelton Lt Col USAF
Air Force Service Chair
Cyber Leadership and Joint Education Department
B.A., University of Texas, San Antonio
M.H.R., Oklahoma University

George J. Trawick
Cyber Security Department
B.S. Columbus State University
M.S. Columbus State University
Ph.D. Auburn University

Thomas Wingfield
Cyber Leadership and Joint Education Department
B.A. Georgia State University
J.D. Georgetown University Law Center
LL.M. Georgetown University Law Center

Harry Wingo
Cyber Security Department
B.S. United States Naval Academy
J.D. Yale Law School

Veronica Wendt
Cyber Leadership and Joint Education Department
B.S. United States Military Academy
M.S. University of Maryland University College

Contact **Information**

STAFF

Aaron Adams
Academic Support/Operations

Gerald Cline-Cole
Academic Support/Operations

Sharron Coleman
Office of Student Services

Clif Ford
Academic Support/Budget

Irem Hatipoglu-Cor
Office of the Chancellor

Jamie Hitaffer
Academic Computing and Classroom Labs

Donald Howell
Academic Computing and Classroom Labs

Nakia Logan
Academic Advising

Constance Marshall
Academic Support/Operations

Charwin Nah
Office of Student Services

Gwen Powell
Academic Support

Nancy Saunders
Office of the Chancellor

George E. Washington
Cyber Strategist/Office of the Chancellor

https://icollege.ndu.edu

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	2090
Dean of Faculty and Academic Programs	3884
Dean of Administration	3885
Office of Student Services	6300
Fax	4860

E-mail: iCollegeOSS@ndu.edu

Department Chairs

Cyber Security	3889
Information, Communication, & Technology	3891
CIO Dept. and CFO Academy	2020
Cyber Leadership & Joint Education	2069
Faculty and Administrative Fax	3974

Mailing Address:

National Defense University
Information Resources Management College
ATTN: Name or Duty Title
300 5th Avenue
Fort McNair, Washington, D.C. 20319-5066

NDU Information Resources Management College
National Defense University
300 5th Ave
Fort McNair, Washington D.C.
20319
202.685.6300

icollege.ndu.edu

NATIONAL DEFENSE UNIVERSITY