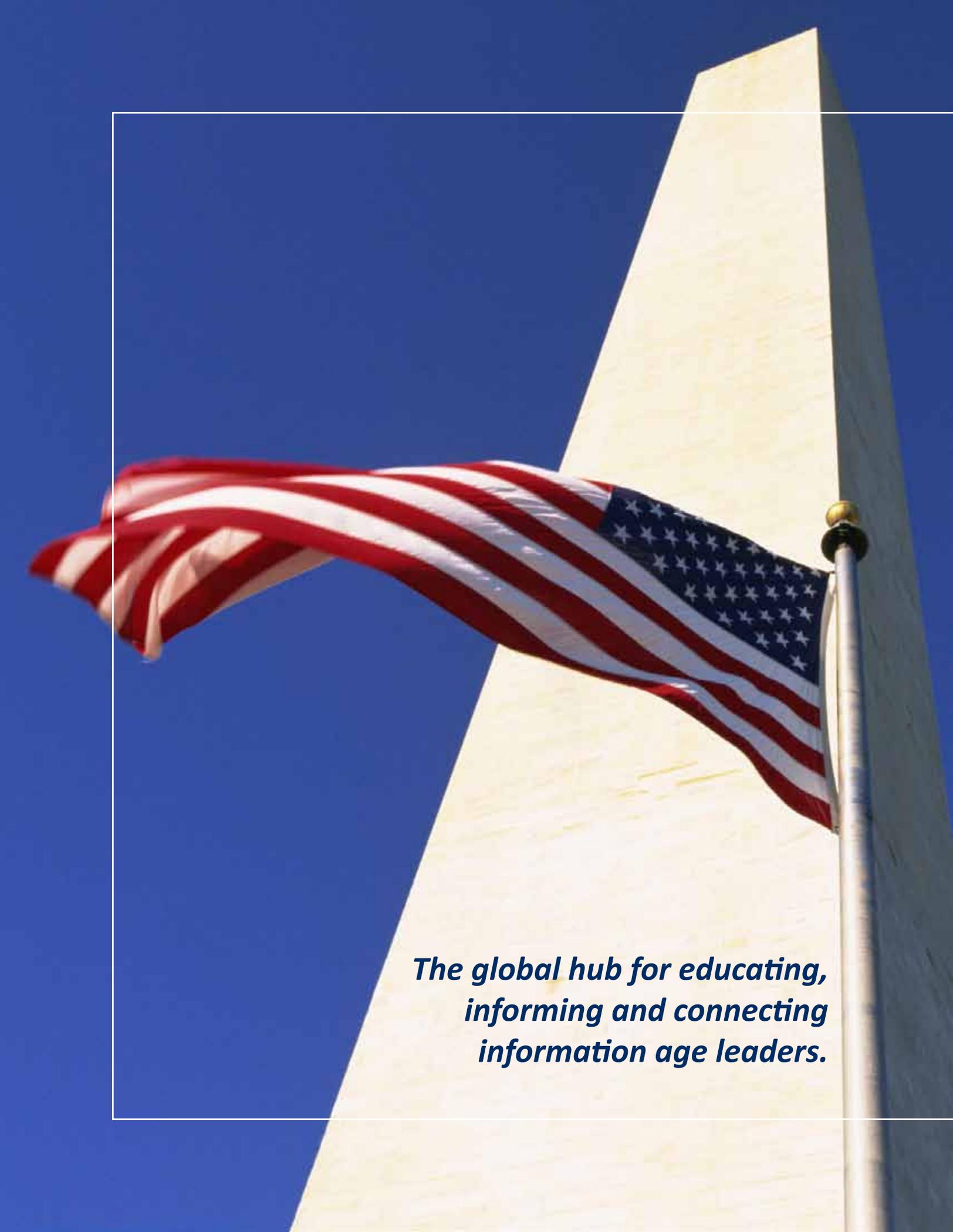


- *Crossing Boundaries*
- *Building Communities*
- *Transforming Organizations*



2009 - 2010
C A T A L O G

An American flag is shown waving in the wind, positioned in front of a large, white, triangular monument. The background is a clear, bright blue sky. The flag's stars and stripes are clearly visible, and the monument's surface has a subtle texture.

*The global hub for educating,
informing and connecting
information age leaders.*

Message from the Senior Director



As we marked our 20th Anniversary last September with a gala at the Gaylord Hotel at the new and magnificent National Harbor, we had an opportunity to reflect on the past and set the pace for the future. The gala brought together over 400 government and academic leaders, private sector collaborators, international partners, and other friends of the College for an evening of networking, testimonials, and renewing old friendships. The history of the IRM College has been one of bringing together diverse groups to solve mutual problems and connect in ways that they could not in other venues. This was our goal when we planned and delivered our Information Leader Symposia Series. Last year, our symposia included Cybersecurity, Privacy, and Government 2.0. These symposia highlighted major topics in the information arena and we are planning to continue these events in the coming year. Our planned symposia for 2009 are “Cloud Computing” and “Web 2.0 Cybersecurity Solutions.” Visit our website often (<http://www.ndu.edu/irmc>) for more details of these events and other things going on at the College.

A new era of government is here; one of transparency, accountability, and accessibility. Our future plans for the College include leading the government in social networking practices, processes, and tools. We want to bring the power of social networking to our students and faculty. Finding ways to educate, inform, and connect people is our vision. Through our Cybersecurity and Innovation and Simulations Laboratories we are using experiential learning techniques to apply conceptual knowledge to real-life situations. In addition, the Telepresence Center will give students, staff, and leadership an intimate, cutting-edge, effective world-wide collaboration tool for a broad range of applications. We are also designing the Collaboration Commons, developed with the NDU library. The Commons will be a learning and experiential space for students and faculty to integrate technologies for communication and collaboration from various realities.

Faculty continued to engage in international activities, expanding our educational capacity-building starting with Bulgaria, Romania, and Sweden. Faculty also worked with the Iraqi government to help them develop their Senior Minister CIOs. The next goal is to cultivate a relationship with Singapore as we cross over the government/private sector boundaries and collaborate with forward-thinking and innovative organizations. Currently, we have established working relationships with more than 30 private sector companies, including Google, Motorola, Northrop Grumman, Tibco, Microsoft, Sprint/Nextel, General Dynamics, SUN Microsystems, Cisco, HP, GeoDecisions, Motorola, Oracle, IBM, VMware, CSC, CSI, and others. Through our connections with the Industry Advisory Council and the American Council of Technology (IAC/ACT), we are collaborating with all levels of government to provide education and networking opportunities. Our relationship with the Armed Forces Communications and Electronics Association (AFCEA), gives us a place to bridge the gap between Defense requirements and industry capabilities. The key here is connecting wherever and whenever possible.

Of course, The College’s outstanding educational programs continue to be updated to address the needs of our students. We cut the ribbon on our Chief Financial Officer (CFO) Academy last September and since then, have been offering a CFO certificate. That program has taken off and we are looking for other arenas to investigate such as the Chief Technology Officer and the Chief Personnel Officer. Our leadership, faculty, and academic programs have been recently honored by AFCEA with the Excellence in IT Award and by ASTD with the 2009 Eagle Award for being a pioneer in distance learning. And we were chosen as one of the Federal 100 award winners for our innovative and progressive programs. We are humbled by these awards but they inspire us to return to the drawing board to address the needs of our students, always remaining agile and responsive. Soon we hope to offer our Government Strategic Leader Master’s of Science Degree.

Indeed, it is a new era of the government. You are invited to join us as we innovate for the future. You can take a course, apply for a certificate program, engage in professional development, or come to our symposia. This is lifelong learning at its best and your participation is welcomed. And if you are an IRM College alumni, let us hear from you. Be sure to join the Association of the IRM College to participate in professional, social, and networking opportunities. Please browse the 2009-2010 Catalog you have in your hands, and contact any faculty or staff member with questions. The IRM College is your College and we hope to see you soon.

Robert D. Childs

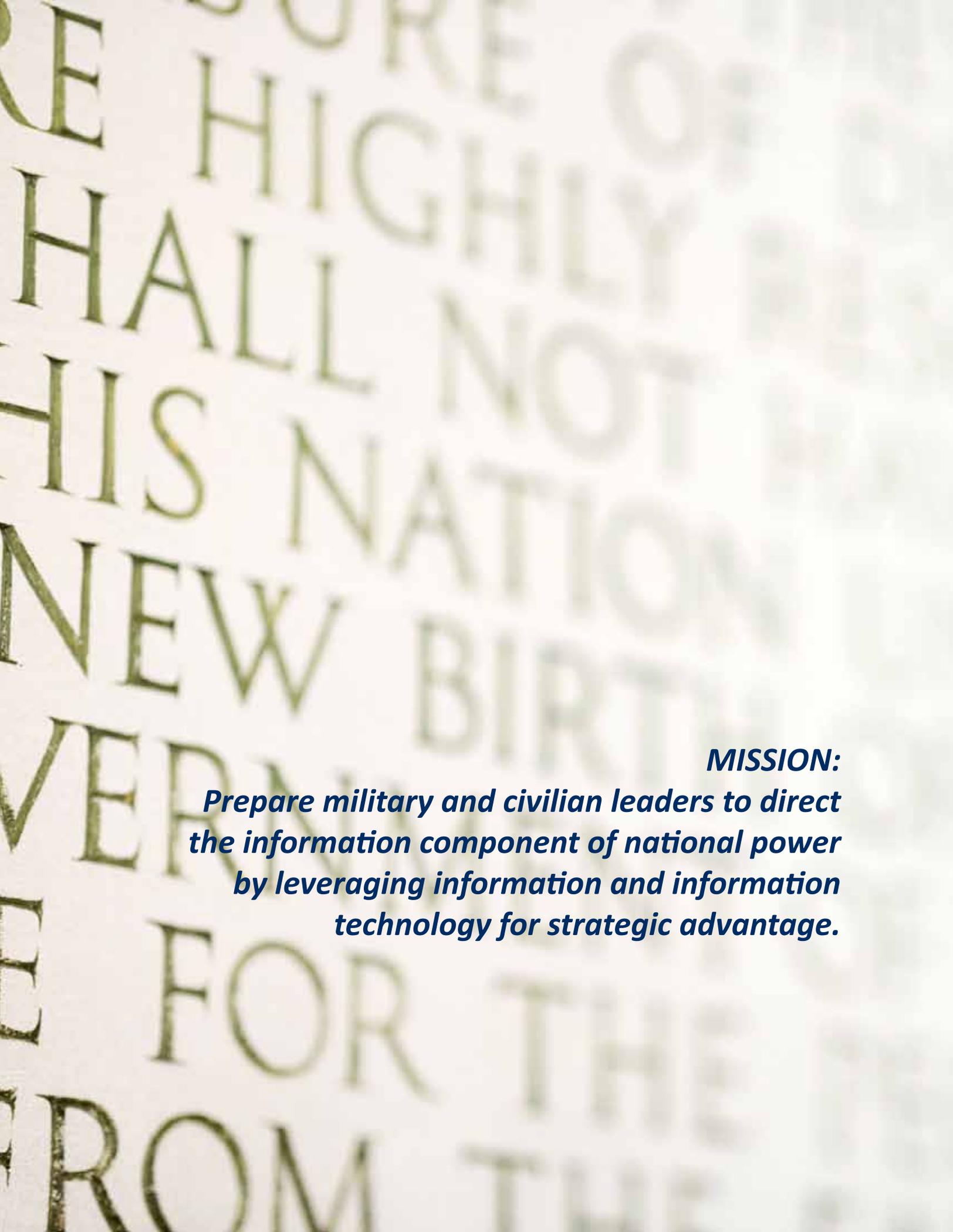
Senior Director, IRM College



*Discover your leadership role in national security.
Explore the Information Resources Management
College's programs and services.*

Contents

Message from Director	1
Overview of College	5
Professional Development Opportunities	10
Degree Program	11
Certificate Programs	
Advanced Management Program (AMP)	14
Chief Information Officer (CIO)	17
Chief Financial Officer Leadership (CFO).....	19
Enterprise Architecture (EA)	21
Government Strategic Leader (GSL)	23
Information Assurance (IA)	24
Information Technology Project Management (ITMP).....	26
Course Descriptions.....	27
Academic Partners	36
Student Services and Policies.....	37
Academic Policies	41
Faculty and Administration.....	44



MISSION:

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

Overview

IRM College Educational Experience



Dr. Mike Piller addresses a class of Japanese students in the Innovation and Simulation Laboratory.

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

Strategic Leader Development for You and Your Organization

The College offers a dynamic range of courses and programs in important information and information resources management topics and issues to develop strategic leaders for the Information Age. Through these educational experiences, information leaders can explore and master the concepts, knowledge, tools, and competencies to transform their organizations. In addition to graduate-

level courses, the IRM College offers all courses for professional development and welcomes students to enroll without seeking a certificate or academic credit. A third option for strategic leader development is "education in context." These educational opportunities include workshops, presentations, forums, and events to develop the government workforce to meet the needs of agencies to accomplish their missions and to develop leaders who can leverage the information component for national security. The College submitted a proposal to the Department of Education in May 2008 to offer a Government Strategic Leader (GSL) Master of Science Degree. The proposed GSL Master's Degree has a core of management and leadership courses focused on the unique challenges and opportunities of defense and government, and a range of concentrations that align with various certificates.

The IRM College 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.

Learning That Is Current, Relevant, and Future-Focused

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

Access to Learning Wherever You Are

To respond to the needs of its learning community, the IRM College offers students opportunities and tools for face-to-face interaction, e-learning, online library resources, and course management software. Classrooms on campus at Fort Lesley J. McNair in Washington, D.C., are equipped with laptop computers for student use during eResident classes. Blackboard (Bb) supports the virtual classroom environment for all students and faculty. Online library resources are available via web access from office and home. 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. The College offers courses in the following formats:

Intensive courses offered either in residence at Fort McNair or by distributed learning for students around the globe.

The **eResident** format uses a blended approach to engage learners in various learning activities:

- Pre-course materials in Blackboard (Bb): Students may access course materials up to 13 days prior to the start date of the course through our online learning platform, Blackboard.
- In-residence portion: Students attend a one-week in-residence portion (see published Schedule of Classes for dates).
- Graded assessment: Students enrolled for certificate/graduate credit must complete an end of course assessment. This typically consists of a paper or project. (The student may engage with the faculty and/or other students virtually for up to three weeks after the in-residence instructional period.)



IRM College Faculty visit Iraq with the Iraqi Team. Dr. Kathleen Schulin (2nd from left), Dr. Teresa Day, (2nd from right), and Dr. Mary McCully (on right).

The **Distributed Learning (DL)** format engages students virtually in 10 to 12 weeks of instruction in Blackboard, use of online library resources, and assignments with faculty and other students.

- Graded assessment portion: Students enrolled for certificate/graduate credit must complete an end-of-course assessment typically consisting of a paper or project. (The student may engage with the faculty and/or other students virtually for up to three weeks after the instructional period.)

The **Advanced Management Program (AMP)**, a 14-week resident program conducted at Fort McNair in Washington, D.C. that leads to the CIO Certificate, CFO Leadership Certificate, or the Government Strategic Leader Certificate.

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

Seminars, symposia, forums, workshops, and other educational activities that faculty conduct to meet particular learning needs of organizations, and to address particular issues and topics.

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



Vivek Kundra, the Federal Chief Information Officer, addresses a packed house at the Cloud Computing Symposium on July 15, 2009 in Lincoln Hall Auditorium.



Information Leader Symposia Series

The Information Resources Management College provides opportunities for students to interact and network with government leaders, practitioners, and scholars in a variety of leading edge topics. These symposia are co-hosted with the Assistant Secretary of Defense (Networks and Information Integration)/DOD/CIO.

SYMPOSIA 2009-2010

The Cloud Computing Symposium
15 July 2009

Web 2.0 Cybersecurity Solutions Symposium
17 November 2009

**Please check our website often for upcoming events:
<http://ndu.edu/irmc>**

The College At a Glance

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

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

The Information Operations and Assurance Department focuses on information operations, assurance, and security in the planning and execution of national and military strategy. The Information Assurance (IA) Certificate Program consists of nested certificates that emphasize security issues and fundamental approaches to the protection of the nation's information infrastructure. The College offers five certificates in IA: National Training Standard for Information Systems Security Professionals (NSTISSI No. 4011), National Information Assurance Training Standard for Senior Managers (CNSSI No. 4012), National Information Assurance Training Standard for System Security Certifiers (NSTISSI 4015), National Information Assurance Training Standard for Risk Analysts (CNSSI 4016), and the Chief Information Security Officer (CISO) Certificate. The Department also sponsors a concentration in Information Operations in the proposed M.S. Degree Program.

The Systems and Technology Department delivers courses and programs focused on successful application of project and program leadership skills, policies, best practices, and tools to acquire and manage an enterprise's information systems, software, and services. Its courses examine IT project and program management, acquisition, enterprise architecture strategies, business

case development, and data management strategies. The Systems and Technology Department delivers the Enterprise Architecture and IT Project Management Certificates with concentrations in the proposed M.S. Degree Program.

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

National Center of Academic Excellence in Information Assurance Education

The IRM College is a National Center of Academic Excellence (CAE) in Information Assurance Education as certified by the National Security Agency and the Department of Homeland Security. The College was originally certified in the year 2000 and subsequently re-certified three times. The College established the Center for Information Assurance Education to conduct education and research focused on concepts and best practices related to information assurance for national security. By playing a leadership role in information assurance strategies, the Center facilitates understanding of the status and practices of information assurance, and conducts and disseminates research on information security, information operations, homeland security, and critical infrastructure protection.

Joint Professional Military Education (JPME)

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

National Security Professional Development (NSPD)

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



Information Resources Management College Faculty and Staff, June 2009.



Dr. Robert Childs (c) accepts the "Excellence in Information Technology" award at the AFCEA Joint Warfighting 2009 Conference from Kent Schneider (l), President and CEO of AFCEA and Paul Cofoni (r), AFCEA's Chairman of the Board.

Picture taken by Michael Carpenter Photography

Professional Development Opportunities

Professional Development Grade

The College welcomes students who wish to enroll in individual courses to learn and to connect with others without seeking a certificate or academic credit. In such cases, we record a grade of Professional Development (PD) in the student's academic record and post it on the official NDU transcript. (Refer to the section on Grading for more information.) Students enrolled in certificate programs may take courses for a PD grade; however, for courses to count toward a certificate, the Master's Degree, or as a prerequisite, students must take them for credit. Students who elect to take coursework for graduate/certificate credit will receive three semester hours of academic credit for each course.

Students electing courses for professional development will:

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

Professional Development Enrollment

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

If you are not already in a certificate program, you may enroll in the IRM College as a Professional Development student through the IRM College website (<http://www.ndu.edu/irmc>).

WHY YOU MIGHT CHOOSE A PROFESSIONAL DEVELOPMENT OPTION:

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



Admiral Rondeau (left), President of National Defense University, talks to Dave Wennergren, the Deputy CIO at the Cloud Computing Symposium on July 15, 2009.

IRM College offers all courses for either graduate/certificate credit or Professional Development (non-credit)

Degree Program

Government Strategic Leader Masters of Science*

The Government Strategic Leader (GSL) Master of Science Degree Program is a selective and competitive program that addresses the educational needs of defense and government leaders who seek to lead complex and diverse 21st Century organizations. Today, even the most seasoned government leaders are facing extraordinary challenges in managing information technology, financial, and human resources, understanding social networks, and competing globally. Information Age leaders must know how to respond to rapidly evolving priorities and how to leverage a multi-generational workforce. They must be agile and adaptable to meet the national security challenges of the future. National security is increasingly recognized as an inter-agency responsibility and not just the purview of the Department of Defense.

The four competencies of: Strategic Thinking, Collaboration and Cross-Boundary Leadership, Leveraging Resources, and Focus on the Enterprise, were adopted by the IRM College as essential for Information Age leaders. In addition to these competencies, IRM College courses develop and faculty hold students accountable for cross-cutting skills and values that must be exemplified by government strategic executives. The curriculum of the GSL Master of Science Degree Program offers a combination of management and leadership intensive courses in a collaborative and interactive environment. Participants from across defense and federal, state, and local government organizations create a learning community where partnerships, information sharing, and network synergies serve as force multipliers.

GOALS OF THE DEGREE PROGRAM

Successful graduates of the Master of Science Degree Program 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 homeland, national, and global security.
- Apply critical and innovative thinking to achieve results-oriented organizational goals.
- Collaborate across boundaries to leverage talent, resources, and opportunities to achieve mission outcomes.
- Create resilient, adaptable, agile, and productive government organizations focused on national security in the Information Age.
- Commit to lifelong development of self and others as reflective learners.
- Lead Information Age defense and government organizations.

DEGREE REQUIREMENTS

The GSL Master of Science Degree requires successful completion of 36 graduate credits. There is no thesis requirement. The Program consists of twelve (12) courses comprised of four components: Foundation, Management, Leadership, and Concentration. Courses in the Government Strategic Leader Certificate (see section on GSL Certificate) form the core of the Master's program. Courses may be taken for the Certificate alone or as the core for the Master's Degree program. Concentrations in the Master's Degree



The GSL core competencies are:

Strategic Thinking, Collaboration and Cross-Boundary Leadership, Leveraging Resources and Focus on the Enterprise.

(Seeking Approval*)

The IRM College is currently seeking approval from the United States Department of Education to award the Government Strategic Leader Master of Science Degree. If and when approval is granted, students will receive graduate credit for the appropriate courses taken from the point of their matriculation. Please visit the IRM College website (www.ndu.edu/irmc) for up-to-date information on the Department of Education approval process, and the College's admission requirements and the application review cycle.

correspond to the College's certificate programs: Chief Information Officer, Chief Financial Officer Leadership, Enterprise Architecture, Information Operations, Information Technology Project Management, and Strategic Transformation (formerly, Organizational Transformation)

Program Completion Time Limit: All coursework applied toward a M.S. degree must be completed within the previous seven years. Students must successfully complete at least one course every 18 months to maintain active status in the program.

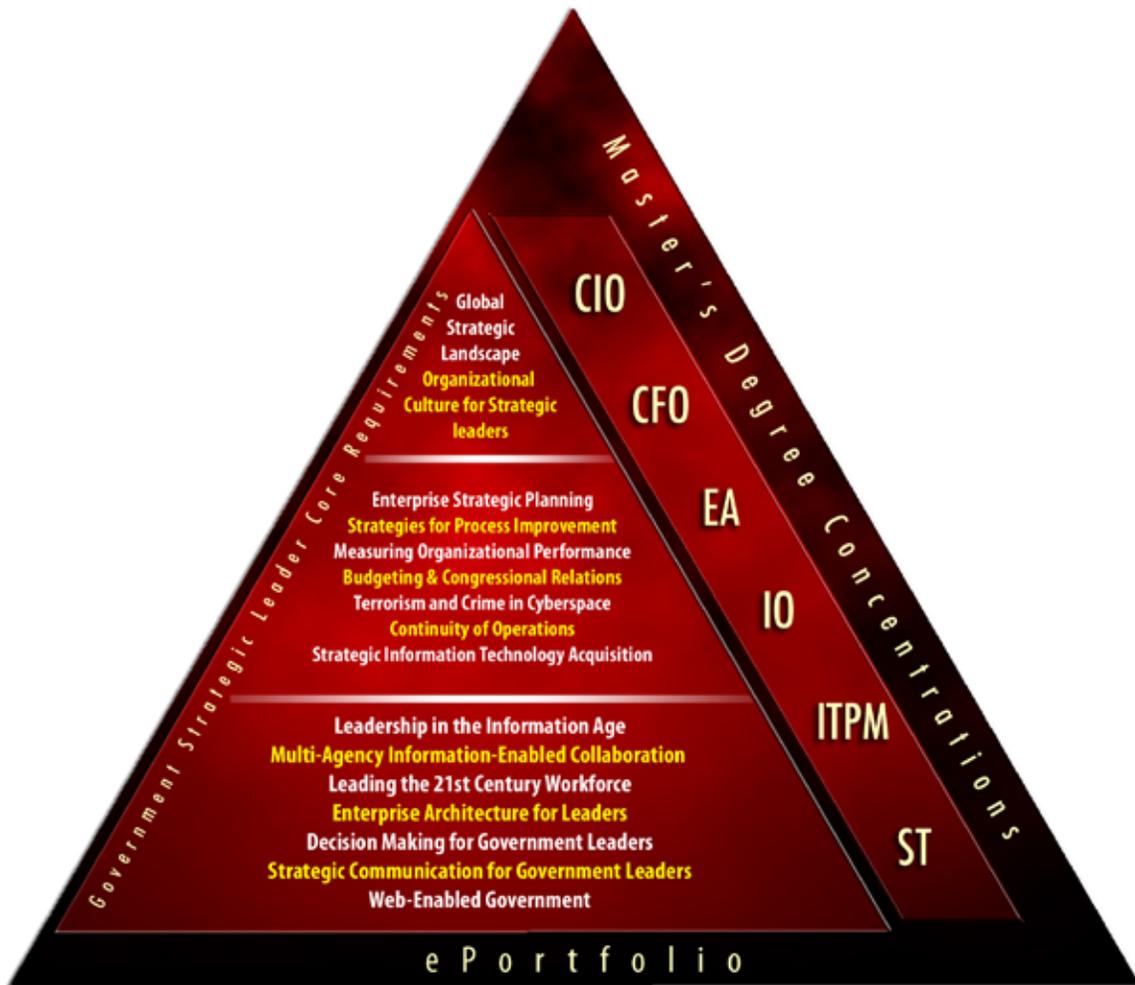
Applying Coursework Earned Prior to Program

Admission: IRM College coursework that has been previously applied to a certificate program also may be used toward the Master of Science Degree. Eligible courses are those that directly fulfill Master of Science Degree requirements. Courses taken for a grade of Audit (AU) or Professional Development (PD), or which have been used to satisfy degree requirements for other advanced degrees are not eligible. All coursework applied toward a M.S. degree must be completed within the previous seven years.

Electronic Portfolio Requirement: Master of Science Degree students are required to complete and present an electronic portfolio (ePortfolio) as part of the degree program of study. The ePortfolio is a personal narrative that documents student learning, reflection, and performance associated with the IRM College Master of Science leadership competencies of: Strategic Thinking, Collaboration and Cross-Boundary Leadership, Leveraging Resources and Focus on the Enterprise.

Admitted Master of Science students will be automatically enrolled in, and must successfully complete, a non-credit asynchronous online seminar, the Leadership Development Seminar (LDS) about the ePortfolio process. The LDS will provide students with guidance on starting and completing the Master of Science ePortfolio. Master of Science ePortfolios must be evaluated a minimum of three times, and at least once per year while students are actively enrolled in the program. Student presentation of a satisfactory ePortfolio to a faculty panel is the final degree requirement.

It is the responsibility of Master of Science students to plan for, submit, and successfully complete all ePortfolio requirements and reviews to fulfill degree requirements and meet program completion deadlines.



GSL M.S. Course List and Concentrations

AI—Information Assurance and Critical Infrastructure Protection

ARC—Enterprise Architecture for Leaders

ASA—Analytics and Simulation for Enterprise Architecture

BBC—Building an IT Business Case

BCP—Budgeting and Congressional Relations for Strategic Leaders

CFF—Changing World of the CFO

COO—Continuity of Operations

CST—Critical Information Systems Technologies

CWC—The Changing World of the CIO

DAC—Defense Enterprise Architecture

DMG—Decision Making for Government Leaders

DMS—Data Management Strategies and Technologies

EAP—Enterprise Architecture Practicum

ESP—Enterprise Strategic Planning

ESS—Enterprise Information Security Risk and Management

FAC—Federal Enterprise Architecture and Advanced Concepts

FFR—The Future of Financial Reporting and Standards

GBE—Government Business Enterprise Transformation

GLS—Global Strategic Landscape

IOS—Information Operations and National Security in the Information Age

IPL—Information Technology Program Leadership

ITA—Strategic Information Technology Acquisition

ITP—IT Project Management

IWS—Information, Warfare, and Military Strategy

JIOPC—Joint Information Operations Planning Course (Offered by the Joint Forces Staff College)

LDC—Leadership for the Information Age

LCW—Leading the 21st Century Workforce

LSI—Leading Strategies for Disruptive Innovation

MAC—Multi-Agency Information-Enabled Collaboration

MEA—Modeling for Enterprise Architecture

MOP—Measuring Results of Organizational Performance

OCL—Organizational Culture for Strategic Leaders

PFM—Capital Planning & Portfolio Management

PMA—Planning and Managing Enterprise Architecture Programs

PRI—Strategies for Process Improvement

RIA—Leadership for Risk Management, Internal Controls, and Auditing

SAL—Software Acquisition Leadership

SCL—Strategic Communication for Government Leaders

SEC—Cyber Security for Information Leaders

SIO—Strategic Infrastructure Operations

TAS—Transformation and Strategic Alignment

TCC—Terrorism and Crime in Cyberspace

WGV—Web-Enabled Government

GSL M.S.	Concentrations					
	(Req) = Required Courses					
	Chief Information Officer	Chief Financial Officer Leadership	Enterprise Architecture	Information Operations	IT Project Management	Strategic Transformation
Courses/Hours	12/36	12/36	12/36	12/36	12/36	12/36
Foundation	GLS OCL	GLS OCL	GLS OCL	GLS OCL	GLS OCL	GLS OCL
Management	3 courses from: MOP (Req) COO ESP ITA PRI	3 courses from: BCP COO ESP MOP PRI	3 courses from: BBC (Req) BCP DMS (Req) PRI MOP WGV	3 courses from: BCP COO (Req) TCC (Req) ESS ESP MOP PRI	3 courses from: BCP COO ESP ITA (Req) MOP PRI TCC	3 courses from: BCP COO ESP MOP PRI TCC
Leadership	3 courses: ARC (Req) DMG (Req) LDC (Req)	3 courses from: ARC DMG LDC LCW MAC	3 courses from: ARC (Req) DMG LDC MAC SCL	2 courses from: ARC DMG LDC MAC SCL (Req)	2 courses from: ARC DMG LDC MAC SCL	4 courses DMG (Req) LCW (Req) MAC (Req) SCL (Req)
Concentrations	2 courses : All (Req) CWC (Req)	4 courses from: BBC CFF (Req) DMS ESS FFR GBE ITP PFM RIA WGV	4 courses : ASA (Req) DAC or FAC (Req) PMA (Req) MEA (Req)	5 courses : IOS (Req) IWS (Req) All or SIO (Req) JIOPC (Req) SEC (Req)	5 courses : BBC (Req) CST (Req) IPL (Req) ITP (Req) SAL (Req)	3 courses GBE (Req) LSI (Req) TAS (Req)
	2 courses from: Any from catalog					

Certificate Programs

Advanced Management Program (AMP)



AMP OFFERINGS:

Academic Year 2010

AMP 39: Sept. 14 – Dec. 18, 2009;
Applications due: Jun. 1, 2009;
Early applications: May 1, 2009

AMP 40: Jan. 25 – Apr. 30, 2010;
Applications due Oct. 1, 2009;
Early applications: Sept. 1, 2009

Academic Year 2011 (Tentative Dates)

AMP 41: Sept. 13 – Dec. 17, 2010;
Applications due Jun. 1, 2010;
Early applications: May 1, 2010

AMP 42: Jan. 24 – Apr. 29, 2011;
Applications due Oct. 1, 2010;
Early applications: Sept. 1, 2010

“Change leadership, collaboration, and communication were very powerful and important leadership competencies woven throughout AMP. The focus on leadership was just right and the laboratories are wonderful resources for students. The IRM College faculty all have passion for their subjects, lessons, and courses.”

The Advanced Management Program (AMP) is a 14-week resident graduate program designed for middle- and senior-level managers who exercise leadership and carry responsibility for promoting and attaining national security, agency, and inter-agency goals through the use of information and/or information technology. The AMP is a highly interactive student-centered educational experience in which strategic thinking, collaboration and cross-boundary leadership, focus on the enterprise, and leveraging resources skills are modeled. AMP students form a learning community that fosters multiple perspectives on a wide range of issues. Students share knowledge and best practices, strive to become better leaders and decision makers, and master the tools of lifelong learning. Interaction with fellow students, faculty, guest speakers, and government executives provides AMP participants with a network of peers throughout the United States, public and private sectors, and internationally.

The graduate-level AMP curriculum core and elective courses provide participants with the option of earning a Chief Information Officer (CIO) Certificate, Chief Financial Officer (CFO) Leadership Certificate, or Government Strategic Leader (GSL) Certificate. Information Assurance Scholarship Program students must select the CIO Certificate concentration and also are required to complete all four courses of the Information Assurance 4011 Certificate.

Chief Information Officer Certificate

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

Chief Financial Officer Leadership Certificate

The CFO Leadership Certificate is designed to develop the next generation of leaders in government financial management. This new certificate leverages the IRM College’s current leadership courses while concentrating on the challenges

and opportunities facing members of the government financial community, including personnel who work in accounting and finance, budget and cost analysis, auditing, and resource management. Refer to the section on the CFO Leadership Certificate for complete information.

Government Strategic Leader Certificate

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

The AMP core courses are:

Policy Foundations of Information

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

Measuring Results of Organizational

Performance (MOP): Provides strategies and techniques for assessing an organization’s performance results as part of strategic planning or budgeting processes. Leverages lessons learned

from inter-agency experience concerning approaches and resources required to establish and validate performance measurement instrumentation, collect and organize performance data, and analyze and report results. Emphasizes mission outcomes in terms of the customer and focuses on information management and technological issues surrounding performance measurement.

Strategies for Process Improvement (PRI): Focuses on strategies, methods, and resources for improving, managing, and controlling processes within and across federal agencies. A senior-level perspective is provided on the tools, techniques, and technologies that enable such strategies. The course emphasizes leadership challenges associated with initiation, collaboration, design, implementation, performance management, and portfolio management of process-centric improvements. *Alternates Fall or Spring with Enterprise Architecture For Leaders (ARC)*

Enterprise Architecture for Leaders (ARC) Examines enterprise architecture (EA) as a strategic capability organizational leaders use for enterprise planning, decision-making, and key process execution. Students explore leadership competencies and management strategies needed to advance EA adoption, use, and institutionalization. Students also explore the

integration of EA with strategic planning, governance, portfolio management, capital planning and investment control, and information assurance. Students examine EA descriptive frameworks and associated models that guide EA development activities and review EA evaluative frameworks used to assess organizational EA management capacities and performance outcomes enabled by the EA. Students further examine challenges to organizational EA adoption, implementation, use, and institutionalization and consider strategies to address them. *Alternates Fall or Spring with Strategies For Process Improvement (PRI)*

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

Refer to the Student Services Section for fees and payment instructions.

In addition to the above core courses, AMP students, as outlined below, complete a total of four required and elective courses to earn certificates in their selected area of concentration.

AMP CIO students are required to complete one (1) additional core courses: *Information Assurance and Critical Infrastructure Protection (All)* and three (3) additional elective courses.

AMP CFO students are required to complete three (3) additional core courses: *Budgeting and Congressional Relations for Strategic Leaders (BCP)*, *The Future of Financial Reporting and Standards (FFR)*, and *Leadership for Risk Management, Internal Controls and Auditing (RIA)*. CFO students must also complete one (1) additional elective course.

AMP GSL students are required to complete two (2) core courses: *Organizational Culture for Strategic Leaders (OCL)* and *Global Strategic Landscape (GLS)*. GSL students must also complete two (2) additional elective courses.

The curriculum map below illustrates the various elements of the AMP.



AMP Application Instructions

Eligibility Requirements

Federal civilian government employees must be at least *GS/GM-12 or equivalent*, and military officers must hold at least *the grade of O-4*. Non-federal students, to include state and local government and private sector employees, must be of an equivalent grade. Private sector employees must be sponsored by a government agency.

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

Application Instructions

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

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

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

State and Local Government and Private Industry:

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

Submit applications to the IRM College Registrar via fax (202-685-4860), e-mail to IRMCRegistrar@ndu.edu, or postal mail to:

IRMC Registrar
300 5th Ave., Bldg. 62
Fort McNair, D.C. 20319-5066

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

Director
Security Assistance Training Field Activity (SATFA)
U.S. Army Training and Doctrine Command
(TRADOC)
ATTN: SATFA-RQ
173 Bernard Road, Bldg. 139
Fort Monroe, VA 23651-1003
DSN: 680-3255
Commercial: (757) 788-3255
Fax: (757) 788-4142
<http://www.satfa.monroe.army.mil/>

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

Questions about AMP admissions or requirements should be addressed to the IRM College Registrar via phone (202-685-6300), or e-mail to IRMCRegistrar@ndu.edu.

Chief Information Officer Certificate Program (CIO)

The Chief Information Officer (CIO) Certificate Program, sponsored by the DOD CIO, is the recognized graduate education for Federal CIO leaders. The CIO Certificate is designed to develop CIO leaders and their agency personnel who can leverage the information component of national power for strategic advantage. The program addresses requirements in the Clinger-Cohen Act (1996), the Government Performance Result Act (1993), the Paperwork Reduction Act (1995), the Federal Information Security Management Act (1996), and the President's Management Agenda (2001). At the end of their program, successful CIO graduates will be able to:

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

Students may apply their certificates, equivalent to at least 15 graduate-level credit hours, towards selected Master's or Doctoral degree programs at several partner institutions of higher education.

CIO Program graduates earn a certificate signed by the DOD CIO and the Director of the IRM College that recognizes they have earned an education in the Federal CIO competencies. The CIO Certificate Program is organized around 12 subject areas directly related to CIO competencies identified by the Federal CIO Council (see the CIO Wheel on the next page). 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 Strategic Leader Master of Science Degree.

Students may apply their certificates, equivalent to at least 15 graduate-level credit hours, toward selected master's or doctoral degree programs at several partner institutions of higher education. See the Academic Partners section of this catalog for more information.

Certificate Requirements

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

- Six core courses in six different competency areas, three of which are required.
- Two other courses of their choice from the College catalog.



CIO HIGHLIGHTS:

Students earn the CIO Certificate by successfully completing eight (8) courses that satisfy the following:

- Six core courses in six different competency areas, three of which are required.
- Two other courses of their choice from the College catalog.

"I am impressed with all of the IRM College professors and their interactive methodology for engaging the class and building teams. I will return to my agency with a concise knowledge of CIO responsibilities, a new vantage point to view my IT department, and a context to understand our successes and failures, and future paths."

CIO Certificate Requirements

Required Core Course (3 courses)		
Key Competency Area	Course/Catalog Number	Title
Policy	CWC (6317)	<i>Changing World of the CIO</i>
Performance- and Results-based Management	MOP (6316)	Measuring Results of Organizational Performance
Security and Information Assurance	All (6203)	Information Assurance & Critical Infrastructure Protection
Additional Core Courses (3 courses from different competency areas)		
Key Competency Area	Course/Catalog Number	Title
Acquisition	ITA (6415)	Strategic Information Technology Acquisition
Architectures and Infrastructures	ARC (6409) DMS (6414)	Enterprise Architectures for Leaders Data Management Strategies and Technologies: A Managerial Perspective
Capitol Planning and Investment	BBC (6430) PFM (6315)	Building an IT Business Case Capital Planning and Portfolio Management
eGovernment / eBusiness	TAS (6528) WGV (6435)	Transformation as Strategic Alignment Web-Enabled Government: Facilitating Collaboration and Transparency
Leadership	LDC (6301) DMG (6323)	Leadership for the Information Age Decision Making for Government Leaders
Process Improvement	COO (6504) PRI (6333)	Continuity of Operations Strategies for Process Improvement
Strategic Planning	ESP (6320) IMP (6318) IWS (6202)	Enterprise Strategic Planning Information Management Planning Information, Warfare, and Military Strategy (Secret clearance required)
Technology Assessment	CST (6510) WGV (6435)	Critical Information System Technologies Web-Enabled Government: Facilitating Collaboration and Transparency
Additional Specialty Courses (2 courses)		
Any Course from the College Catalog		



Chief Financial Officer Leadership Certificate Program (CFO)

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 National Defense University's Information Resources Management College. The CFO Academy offers graduate-level courses and services for middle- to senior-level personnel in the government financial management community to prepare them to create and lead 21st Century government organizations.

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

Courses in the CFO Leadership Certificate are conducted in the eResident format in classrooms at National Defense University at Fort McNair. The eResident courses engage students for five weeks: one week of pre-reading and assignments, five days of class in residence (8 AM to 5 PM Monday through Friday), and three weeks to complete graded academic assignments as assigned by the course leader. Most, and eventually all, of the courses in the program are also offered in an on-line (distributed learning) format that requires 10 to 12 weeks of asynchronous work plus three weeks to complete graded academic assignments.

Eligibility Requirements

Financial management knowledge can be verified by having earned a bachelor's degree or master's degree in a business-related field, or a C.P.A., Certified Defense Financial Management (CDFM), or Certified Government Financial Management (CGFM). For those who do not meet the criteria for financial management knowledge, a two-course probationary period of admission can be approved while students are seeking the CDFM or CGFM.

Graduates of the CFO Leadership Certificate will be able to:

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

Certificate Requirements

To earn the CFO Leadership Certificate students must successfully complete eight graduate-level courses. Four courses must be taken from the Strategic Finance category, one of which, *The Changing World of the CFO*, is required. Three of the Strategic Finance courses, *The Changing World of the CFO*, *The Future of Financial Reporting and Standards*, and *Leadership for Risk Management, Internal Controls, and Auditing*, are only open to students enrolled in the CFO Leadership Certificate. Students must also select four courses from the Leadership category. Courses may be taken in any order.

The CFO Leadership Certificate is also a concentration in the proposed IRM College Government Strategic Leader Master of Science Degree Program (seeking approval from the U.S. Department of Education). The IRM College is working with its academic partner universities across the U.S. to accept the CFO Leadership Certificate as 15 graduate credits toward selected Master's and doctoral degree programs at selected institutions.



ELIGIBILITY REQUIREMENTS:

- At least O-5 or GS-14 or equivalent
- Bachelor's Degree
- At least three years of financial management experience
- Documented knowledge of financial management, and leadership potential as noted by nominator

***"Wow!
The IRM College assembled a tremendous collection of regular faculty and guest instructors for the Changing World of the CFO Course. The Course is everything I expected and more. I'm excited about the remainder of the program."***



CFO Certificate Requirements

Required Core Courses	
Course/ Catalog Number	Course Title
CFF (6601)	<i>Changing World of the CFO</i>
Strategic Finance Courses (3 courses)	
Course/ Catalog Number	Course Title
BCP (6417)	<i>Budgeting and Congressional Relations for Strategic Leaders</i>
DMG (6323)	<i>Decision Making for Government Leaders</i>
FFR (6602)	<i>The Future of Financial Reporting and Standards</i>
GBE (6501)	<i>Government Business Enterprise Transformation</i>
PFM (6315)	<i>Capital Planning & Portfolio Management</i>
RIA (6603)	<i>Leadership for Risk Management, Internal Controls, and Auditing</i>

Leadership Courses (4 courses)	
Course/ Catalog Number	Course Title
ARC (6412)	<i>Enterprise Architecture for Leaders</i>
BBC (6430)	<i>Building an IT Business Case</i>
COO (6504)	<i>Continuity of Operations</i>
DMS (6414)	<i>Data Management Strategies and Technologies</i>
ESP (6320)	<i>Enterprise Strategic Planning</i>
ESS (6206)	<i>Enterprise Information Security & Risk Management</i>
ITP (6416)	<i>IT Project Management</i>
LCW (6506)	<i>Leading the 21st Century Workforce</i>
LDC (6301)	<i>Leadership for the Information Age</i>
MAC (6512)	<i>Multi-Agency Information-Enabled Collaboration</i>
MOP (6316)	<i>Measuring Results of Organizational Performance</i>
OCL (6321)	<i>Organizational Culture for Strategic Leaders</i>
PRI (6333)	<i>Strategies for Process Improvement</i>
WGV (6435)	<i>Web-Enabled Government</i>

Enterprise Architecture (EA) Certificate Program

Enterprise Architecture (EA) is at the heart of agencies' ability to achieve performance objectives through optimizing business processes and investing effectively in information systems. Highly skilled EA strategists and practitioners are required to create and maintain the EA. The Information Resources Management College's graduate-level Enterprise Architecture (EA) Certificate Program prepares architects with the leadership, policy, and technical competencies required for the three levels of EA responsibilities recently identified by the Office of Personnel Management.

Beginning in October 2009, the IRM College's EA programs consist of three certificates (Architect, Enterprise Architect, and Chief Enterprise Architect). Each certificate consists of four courses, three required and one concentration. They are delivered in either eResident or distributed learning format.

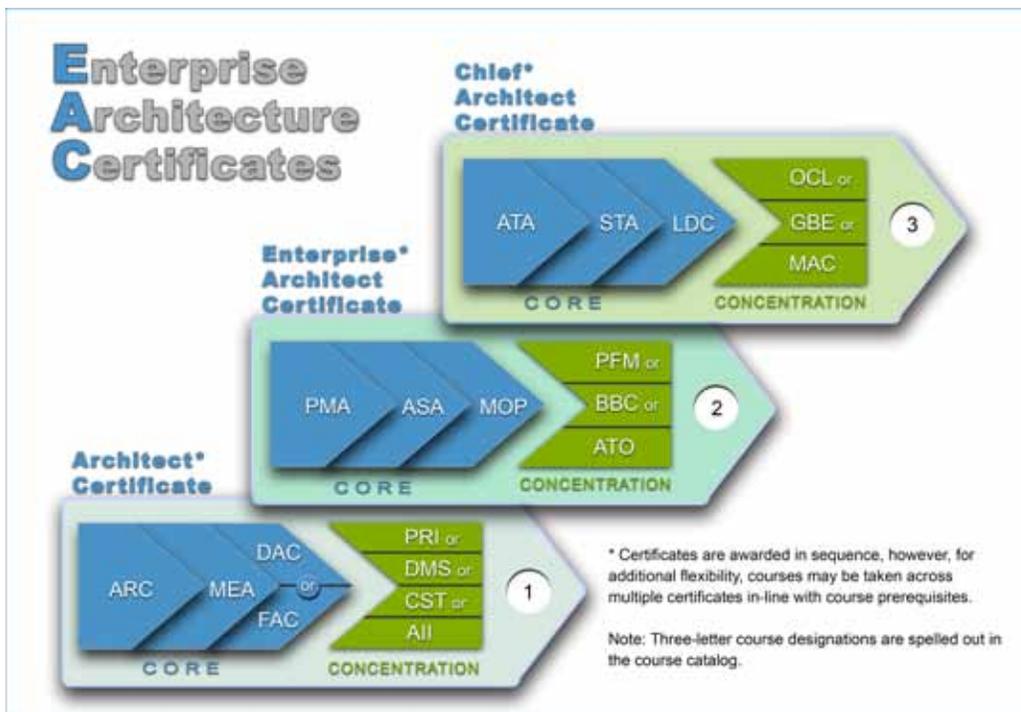
Government leaders who successfully complete the program are empowered to:

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



EA CURRICULUM HIGHLIGHTS:

The IRM College's EA program consists of three certificates, reflecting increasing mastery of enterprise architecture technical and leadership skills. Each certificate requires successful completion of four courses to master the competencies at an appropriate level identified by the OPM 2210 Job Family Standard, Federal CIO Council, and the DOD EA Competency Framework.



"An enterprise architecture (EA) is a blueprint that describes an organization's or a functional area's current and desired state in both logical and technical terms, as well as a plan for transitioning between the two states. As such, it is a recognized tenet of organizational transformation and IT management in public and private organizations."

— GAO, 2008

The certificates document increasing mastery of enterprise architecture technical and leadership skills. The three levels are:

Architects focus on the development of architectures.

Their primary function is to develop architectures based on user requirements and input from subject matter experts. As Architects mature, their experience includes the use of various modeling techniques and tools or enterprise-level architecture development.

Enterprise Architects focus on the analysis and management of architectures. Their primary function is to analyze architectures for the purposes of integration, interoperability, gap analysis, risk assessment, leveragability, compliance, and business decision making. In addition to the analytics, they manage the architecture program. As Enterprise Architects mature, their experience includes the use of various analysis techniques and programs, or enterprise-level analysis and leading areas within EA programs.

Chief Enterprise Architects focus on leading organizational transformation through the discipline of EA. Their primary function is to lead an architecture effort through its entire lifecycle, from initiation to development to execution and implementation. As Chief Enterprise Architects mature, their experience includes strategic analysis, transformation efforts, communication, and leadership of an enterprise-level architecture.

Generally, courses may be completed in any order. A few courses have prerequisites; however, before being awarded the next level certificate, the student must successfully complete the four courses for it and all courses required for any prior level certificates. As

each certificate is completed, graduates grow in their knowledge and ability to lead the application of a variety of approaches, methods, techniques, and work products to facilitate cross-boundary leadership, such as:

- Department of Defense’s Architecture Framework (DODAF), Global Information Grid (GIG), and the Defense Information Enterprise Architecture.
- Office of Management and Budget (OMB) and the CIO Council’s Federal Segment Architecture Methodology (FSAM), Federal Enterprise Architecture (FEA) Reference Models, the Federal Enterprise Architecture Framework (FEAF)
- Industry-based EA frameworks (e.g., Zachman and TOGAF)

In combination with other IRM College coursework, students may earn a Master of Science degree with a concentration in Enterprise Architecture. See the M.S. section of this catalog for more information.

Students enrolled in and graduated from the current EA Certificate who wish to earn the new certificates will be advised on a case-by-case basis.

“Effective Enterprise Architects must be proficient in a myriad of competencies ranging from transformational leadership and communication to envisioning desired organizational and technology capabilities. These are not easy feats to accomplish, which is why great enterprise architects are in demand.”

— CIO Magazine, 2007



“Vivek Kundra (l), the Federal CIO, Dave Wennergren (c), the Deputy DOD CIO, and Admiral Rondeau (r), the NDU President, enjoy the Cloud Computing Symposium on July 15, 2009 along with a packed auditorium in Lincoln Hall.”

Government Strategic Leader (GSL) Certificate Program



Today, even the most seasoned government leaders are facing extraordinary challenges in managing resources, information and communication technologies, social networks, and globalization. As strategic leaders, they must respond to rapidly evolving national priorities and a dynamic environment.

The IRM College's Government Strategic Leader Certificate provides government leaders and managers with the essential tools and strategies required to lead dynamic, complex, and diverse 21st Century organizations.

The curriculum engages participants in understanding their organization's unique role and those of other organizations, and how to collaborate to achieve

organizational, inter-agency, and national mission and goals. Participants form a learning community to share knowledge, analyze and leverage strategic resources (human, technological, and financial), and create and articulate a vision for themselves and their organizations.



GSL CURRICULUM HIGHLIGHTS:

The IRM College's Government Strategic Leader Certificate provides government leaders and managers with the essential tools and strategies required to lead dynamic, complex, and diverse 21st Century organizations.

"Very useful information that I can start using today. High quality education like this is difficult to get."

Certificate Requirements

To earn the Government Strategic Leader Certificate, students must complete eight (8) graduate-level courses that may be taken in any order. Two (2) foundation courses are required that focus on organizational clients and culture, and the dynamic landscape of government and security. Students select three (3) additional courses in management and three (3) in leadership to meet their professional and/or organizational needs.

Required Courses (2 courses)	
Course/Catalog Number	Course Title
GLS (6213)	Global Strategic Landscape
OCL (6321)	Organizational Culture for Strategic Leaders
Required Courses (2 courses)	
Course/Catalog Number	Course Title
BCP (6147)	Budgeting and Congressional Relations for Strategic Leaders
COO (6504)	Continuity of Operations
ESP (6320)	Enterprise Strategic Planning
ITA (6415)	Strategic Information Technology Acquisition
MOP (6316)	Measuring Results of Organizational Performance
PRI (6333)	Strategies for Process Improvement
TCC (6215)	Terrorism and Crime in Cyberspace
Leadership Courses (3 courses)	
Course/Catalog Number	Course Title
ARC (6412)	Enterprise Architecture for Leaders
DMG (6323)	Decision Making for Government Leaders
LCW (6506)	Leading the 21st Century Workforce
LDC (6301)	Leadership for the Information Age
MAC (6512) (required)	Multi-Agency Information-Enabled Collaboration
SCL (6322)	Strategic Communication for Government Leaders
WGV (6435)	Web-Enabled Government

Information Assurance (IA) Programs



IA CURRICULUM HIGHLIGHTS:

The Committee on National Security Systems (CNSS) has certified the curriculum offered by the Information Resources Management (IRM) College as compliant with the following national IA education and training standards:

- 4011: IS Security Professionals
- 4012: Senior Systems Managers
- 4015: System Certifiers
- 4016: Risk Analysts

“Cybersecurity is not just a buzzword in my line of work. After this program, I can look at the prospect of change with enthusiasm, embrace it and, hopefully, in the process I can influence my organization’s processes and its leaders.”

The Information Assurance (IA) Program consists of several certificates that prepare graduates to:

- Exercise strategic leadership in the development and use of information security strategies, plans, policies, enabling technologies, and procedures;
- Develop and lead programs to provide information security controls, 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 IA decisions; and
- Develop and lead, in accordance with laws and regulations, an enterprise IA program that promotes and attains national security, agency, and interagency goals.

The Committee on National Security Systems (CNSS) has certified the curriculum offered by the Information Resources Management (IRM) College as compliant with the following national IA education and training standards:

- NSTISSI 4011 for Information Systems Security Professionals.
- CNSSI 4012 for Senior Systems Managers includes the Chief Information Officer (CIO), Designated Approving Authority (DAA), and Chief Technology Officer (CTO).

- NSTISSI 4015 for System Certifiers.
- CNSSI 4016 for Risk Analysts.

Although the IA certificates do not qualify as a certification under DOD 8570.1-M, The IA Workforce Improvement Program, they do help prepare graduates for commercial certifications listed in DOD 8570.1-M. In addition to DOD 8570.1-M commercial certification requirements, DOD personnel who perform IA functions on national security systems are required to meet CNSS training requirements. The certificates satisfy that CNSS requirement.

The Chief Information Security Officer (CISO) Certificate is a source of graduate-level information security education for Senior Agency Information Security Officers (SAISO), their staffs, and information assurance managers. This certificate provides education to respond to the requirements set forth in the Federal Information Security Management Act (FISMA).

Students may apply their certificates, equivalent to at least nine graduate-level credit hours, toward selected Master’s or doctoral degree programs at several partner institutions of higher education. Students should begin the certificates by first taking the All and GEN courses, followed by SEC and ESS. Successful completion of three (3) of these four (4) courses may be applied toward requirements for the CIO Certificate. Students in the Advanced Management Program have the opportunity to qualify for the 4011 certificate.



Information Assurance NSTISSI No. 4011 Certificate Requirements

Required Courses (4 courses)	
Course/Catalog Number	Course Title
All (6203)	<i>Information Assurance and Critical Infrastructure Protection</i>
ESS (6206)	<i>Enterprise Information Security and Risk Management</i>
GEN (6205)	<i>Global Enterprise Networking and Telecommunications</i>
SEC (6201)	<i>Cyber Security for Information Leaders</i>

Information Assurance CNSSI 4012, 4016, and Information Assurance NSTISSI 4015 Certificate Requirements

Required Courses (5 courses)	
Course/Catalog Number	Course Title
All (6203)	<i>Information Assurance and Critical Infrastructure Protection</i>
ATO (6209)	<i>Approval to Operate: Information System Certification & Accreditation</i>
ESS (6206)	<i>Enterprise Information Security and Risk Management</i>
GEN (6205)	<i>Global Enterprise Networking and Telecommunications</i>
SEC (6201)	<i>Cyber Security for Information Leaders</i>

CISO Certificate Requirements

Required Courses (7 courses)	
Course/Catalog Number	Course Title
All (6203)	<i>Information Assurance and Critical Infrastructure Protection</i>
ATO (6209)	<i>Approval to Operate: Information System Certification & Accreditation</i>
CBL (6204)	<i>Cyberlaw</i>
COO (6504)	<i>Continuity of Operations</i>
ESS (6206)	<i>Enterprise Information Security and Risk Management</i>
GEN (6205)	<i>Global Enterprise Networking and Telecommunications</i>
SEC (6201)	<i>Cyber Security for Information Leaders</i>
Additional Specialty Courses (2 courses)	
Course/Catalog Number	Course Title
CIP (6212)	<i>Protection of Critical Infrastructure and Key Assets</i>
HST (6503)	<i>Homeland Security Tools & Techniques</i>
IOS (6207)	<i>National Security in the Information Age</i>
IWS (6202)	<i>Information, Warfare, and Military Strategy</i>
SIO (6214)	<i>Strategic Infrastructure Operations**</i>
SPA (6508)	<i>Privacy Rights and Challenges in the Information Age</i>
SCS (6210)	<i>Managing Security of Control Systems</i>
TCC (6215)	<i>Terrorism and Crime in Cyberspace</i>

Information Technology Project Management (ITPM) Certificate Program



ITPM CERTIFICATION:

***Project Management Professional (PMP) certification** is offered by the Project Management Institute. Certification requires completion of a formal competency examination. Examination candidates must present evidence of having specified levels of general education and project experience and having successfully completed at least 35 contact hours of project management education. Details are available at the PMI website at: <http://www.pmi.org>.

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

The ITPM Certificate develops project management competencies in three dimensions: project leadership skills, IT program/project management concepts and methods, and IT issues and developments. These competencies provide the knowledge,

skills, and abilities identified by the CIO Council and OPM for IT project managers. In an integrated set of courses, students learn IT project management policies, regulations, theories, and concepts; how to apply best practices using actual IT program examples and case studies; and how to select and apply state-of-the-art IT project management tools. The ITPM Certificate is a specialty in the Government Strategic Leader Master of Science Degree.

Certificate Requirements

Award of the Information Technology Project Management Certificate requires successful completion of four (4) core courses and two (2) specialty courses. The core courses are *Strategic Information Technology Acquisition (ITA)*, *Critical Information Systems Technologies (CST)*, *Building an IT Business Case (BBC)*, and *Information Technology Project Management (ITP)*. Two specialty courses are required: *Software Acquisition Leadership (SAL)* and *Information Technology Program Leadership (IPL)*. There are currently no prerequisites for the courses listed in the table below.

ITPM Curriculum Map

Core Courses			
Strategic IT Acquisition (ITA)	Critical Information Systems Technologies (CST)	Building an IT Business Case (BBC)	Information Technology Project Management (ITP)
Specialty Courses			
Information Technology Program Leadership (IPL)		Software Acquisition Leadership (SAL)	

ITPM Certificate Requirements

Required Core Courses (4 courses)	
Course/Catalog Number	Course Title
BBC (6430)	<i>Building an IT Business Case</i>
CST (6510)	<i>Critical Information Systems Technologies</i>
ITA (6415)	<i>Strategic Information Technology Acquisition</i>
ITP (6416)	<i>Information Technology Project Management</i>
Additional Specialty Courses (2 courses)	
Course/Catalog Number	Course Title
IPL (6411)	<i>Information Technology Program Leadership</i>
SAL (6410)	<i>Software Acquisition Leadership</i>

"I am very pleased with my experiences as a student at the IRM College. Thanks to the excellent staff and faculty, I have decided to pursue a Masters from the IRM College in addition to the CIO and ITPM certificates."

All—Information Assurance and Critical Infrastructure Protection (6203)

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

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

ARC—Enterprise Architecture for Leaders (6412)

This course examines enterprise architecture (EA) as a strategic capability organizational leaders use for enterprise planning, decision-making, and key process execution. Students explore leadership competencies and management strategies needed to advance EA adoption, use, and institutionalization. Students also explore the integration of EA with governance, strategic planning, budgeting, capital planning, portfolio management, and information assurance. Students examine EA descriptive frameworks and associated models that guide EA development activities and review EA evaluative frameworks used to assess organizational EA management capacities and performance outcomes enabled by the EA. Students further examine challenges to organizational EA adoption, implementation, use, and institutionalization and consider strategies to address them.

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

ASA—Analytics and Simulation for Enterprise Architecture (6436)

Prerequisites: DAC or FAC

This course examines analytical and simulation techniques to evaluate an organization's Enterprise Architecture (EA) for strengths, weaknesses, opportunities and threats to improve organizational performance. A four-phase analytical strategy provides the overall direction of the course using baseline integrity evaluation, baseline profile and gap analysis, target and gap analysis, and implementation plan dependency, sizing and capacity evaluation. Additional topics include the use of analytics to validate the quality and completeness of data collection strategies and the use of simulation techniques to evaluate the completeness of static models and alternatives. Students gain hands-on experience through the use of an automated EA repository and analytic tools to support analysis.

Learning Outcomes: Students will be able to leverage automated tools and analytical techniques to evaluate EA repository tool content and identify opportunities for improved organizational performance.

ATA—Advanced Strategies in Enterprise Architecture (6437)

Prerequisites: Completion of Level II courses

This course examines advanced strategies and topics in enterprise architecture (EA) building upon and integrating prior academic experiences with the student's experience as Enterprise Architecture (EA) practitioner. Alternative EA Governance strategies and integration used in industry and public sector will be examined. Through an overview approach, students evaluate the OMB Exhibit 300 to determine architectural alignment with an organization's EA and to assist program sponsors in developing the Exhibit. Analytical techniques and automated tools will be used to evaluate the IT portfolio trade-off analysis with respect to the target architecture and transition plan. Students will explore the supporting relationship of EA and an organization's strategic plan. Students will further evaluate organizational theoretical constructs for improved mission performance in the Information Age. Finally, agile organizational characteristics will be considered as part of an in-depth exploration of Federated EA concepts.

Learning Outcomes: Students will be able to improve the effectiveness of the EA and EA program's contribution to mission performance through improved governance and organizational design strategies. This course won't be offered until the 2010-2011 academic year.

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 individual roles, responsibilities, documentation, and reporting requirements required to support the Designated Accrediting Authority (DAA)/Authorizing Official (AO) in approving the classification level of an information system and granting ATO at a specified level of trust. The course provides an overview of Department of Defense and federal department and agency certification and accreditation processes (e.g., Defense Information Assurance Certification and Accreditation Process; National Institute of Standards and Technology (NIST) risk management framework process), acquisition management, and system security architecture considerations.

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

BBC—Building an IT Business Case (6430)

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

Course Descriptions

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

BCP—Budgeting and Congressional Relations for Strategic Leaders (6417)

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

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

CBL—Cyberlaw (6204)

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

Learning Outcomes: Students will be able to (1) assess potential legal issues that might flow from implementing and not implementing information security policies, practices, and procedures, and (2) create policies and operating procedures for an organization that are ethically and legally sound.

CFF—Changing World of the CFO (6601) For CFO Certificate students only

This course focuses on the changing environment for the federal Chief Financial Officer (CFO). The course provides an overview of the essential elements of the current and future roles of government CFO and their staffs. It surveys the various roles of the executive and strategic leader, compliance officer, risk manager, transaction processor, strategic planner, fiduciary reporter, and reporter of management and financial information. The course discusses the policies, challenges and opportunities associated with decision support, business process improvement, systems integration, financial systems, ethics, workforce development, performance management, budget, and portfolio management. Standards, privacy, and transparency issues are considered and discussed. The fundamental role of the networked community as the critical ingredient of success is explored in depth.

Learning Outcomes: Students will be able to: (1) analyze the most pressing governance issues relevant to leading financial transformation in government.; (2) evaluate the philosophical perspectives, roles & dynamic relationships of the appropriate organizations and functional areas (such as budgeting, accounting, auditing, compliance and planning) impacting the financial community decisions; and (3) create and communicate a convincing case (resource requirements, prioritization documents, etc) that can lead to strides in financial transformation in government.

CIP—Protection of Critical Infrastructures and Key Assets (6212)

This course provides a foundation for analysis of strategies, policies, critical infrastructure plans, investments, and management challenges in protecting the national critical infrastructures and key assets. It examines various approaches for protecting critical infrastructures and a framework for prioritizing protection initiatives. Benefits of reducing risks, lessening vulnerabilities, deterring threats, and minimizing the consequences of terrorist attacks as well as man-made and natural disasters are explored. Other topics include an examination of the significant synergy required between the private and public sectors in homeland security and homeland defense, the importance of protecting the IT infrastructure as a foundation of all critical infrastructures, and implementation strategies for infusing policies and plans in government organizations.

Learning Outcomes: Students will be able to (1) analyze national strategies, public policies, and prospective homeland security critical infrastructure plans; (2) compare and contrast the strengths and weaknesses of various approaches established for the protection of critical infrastructures and key resources; and (3) create a strategy that incorporates homeland security and defense policies and plans for protection of a critical infrastructure and its corresponding key assets.

COO—Continuity of Operations (6504)

This course provides a broad description of the major elements involved in developing and implementing effective continuity of operations plans for government agencies. Using Federal regulations policies as a backdrop, the course examines the technological, human capital, legal, and acquisition factors involved in creating and maintaining a continuity of operations plan. Topics include determining key assets and systems, creating and implementing emergency plans, working with the responder community, developing metrics and exercises, and restoring effective operations.

Learning Outcomes: Students will be able to analyze problems stemming from the absence of a comprehensive, tested continuity of operations plan, and create a strategy to develop and implement such a plan.

CST—Critical Information Systems Technologies (6510)

This course probes the rapid advances in all aspects of information systems technology from the perspective of both the functional and the information resources manager. The course provides an overview of both the current state of the art and the trends in information systems technology with particular attention to software development technologies, data management, computer systems hardware, human-computer interfaces, voice recognition, natural language understanding, collaborative technologies, telecommunications technologies, and electronic commerce technologies. It concludes with a group exercise designed to determine how a CIO can address the issues these technologies introduce within an organization.

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

CWC—The Changing World of the CIO (6317)

This course explores the changing role of the Chief Information Officer in Federal agency and inter-agency information activities. Based upon current Federal statutes and policy directives, the course examines the CIO's explicit and implicit information, technology and business roles. Students focus on developing and implementing policy guidance while playing the role of a CIO. Students also learn how to leverage best practices to plan, acquire, manage, and use information resources in a dynamic global environment so as to improve agency mission performance and citizen service delivery.

Learning Outcomes: Students will be able to analyze the role of the CIO in agency and inter-agency information leadership activities and will be able to create an organizational information resources management program that is based upon current Federal policy guidance in a multi-agency information sharing environment.

DAC—Defense Enterprise Architecture (6438)

Prerequisite: MEA

This course presents policies, practices, and strategies to develop and implement enterprise architectures (EA) supporting Department of Defense (DOD) organizations. Students examine in greater detail the DOD Architecture Framework (DODAF) and associated work-products, first introduced in the Modeling for Enterprise Architecture course. Additionally, students explore the DOD Defense Information Architecture and Business Enterprise Architecture (BEA). Aspects of the Global Information Grid (GIG), such as the net-centric data strategy, are explored. The course concludes with an overview of the Office of Management and Budget's direction on developing and implementing EA, with a primary focus on the Federal Segment Architecture Methodology.

Learning Outcomes: Students will be able to assess the degree to which an agency's enterprise architecture is consistent with the DOD Architecture Framework, and recommend appropriate EA development, implementation, sustainment, or governance strategies. They will also be able to recommend strategies for responding to the Office of Management and Budget's EA segment reporting requirements using a DOD Architecture Framework.

DMG—Decision Making for Government Leaders (6323)

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

Learning Outcomes: Students will be able to analyze leadership decision making and the decision environments in federal government agency and interagency settings; assess the challenges and opportunities for decision makers in federal government collaborative and information-sharing environments; assess decision conse-

quences and outcomes in terms of agency missions, political mandates, and statutory guidance; and determine the types of decision tools appropriate for their organization.

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

This course explores data management and its enabling technologies as key components for improving mission effectiveness through the development of open, enterprise-wide, and state-of-the-art data architectures. It examines management issues such as the implementation of the data component of the Enterprise Architecture specified by OMB. In addition, 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. Case studies allow students to explore data management issues and implementation. While geared for managers, the course provides sufficient insight into the underlying technologies to ensure that students can evaluate the capabilities and limitations of data management options and strategies.

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

EAP—Enterprise Architecture Practicum (6413)

Prerequisite: IMP, PRI, ARC, DMS, PMA, GIG or FAC as well as an approved project proposal.

As the Enterprise Architecture (EA) Program capstone course, this course engages students in an integrated application of principles, policies, and practices of the EA Certificate Program. Students will identify enterprise architecture issues, conduct research, develop and assess solution strategies, and then present the executed strategies in the context of an intensive case study based upon the actual experience of a government agency.

Learning Outcomes: Students will be able to evaluate the state of an agency's EA development effort and propose, assess, and select strategies to develop and implement an EA successfully. They will be able to explain and justify their recommendations regarding EA development clearly and authoritatively through position papers and oral presentations.

ESP—Enterprise Strategic Planning (6320)

This course conducts a strategic assessment by reviewing the various elements of The National Security Strategy of the United States of America (information, economic, diplomatic, and military power) and supporting strategies (e.g., National Strategy for Homeland Security, National Strategy for Combating Terrorism, National Defense Strategy, National Military Strategy, etc.) to understand the strategic direction of the Federal Government and its impact on their organization. They will review and critique the U.S. national security and inter-agency strategic planning process and explain the unique role that each agency plays in achieving inter-agency and national missions and goals. Students will explain various approaches to strategic planning in the face of uncertainty.

Learning Outcomes: Students will be able to assess an existing National Strategy, a government agency strategic plan, or a government agency component strategic plan, and recommend appro-

Course Descriptions

priate changes to improve the robustness of these existing plans against potential futures.

ESS—Enterprise Information Security and Risk Management (6206)

This course explores three themes based on the Certified Information Security Manager® (CISM®) 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, students analyze 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 then concentrates on the challenges of implementing risk management and governance through enterprise security/assurance program management. This includes enterprise information and cyber security strategies, policies, standards, controls, measures (security assessment/metrics), incident response, resource allocation, workforce issues, ethics, roles, and organizational structure.

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

FAC—Federal Enterprise Architecture (6409)

Prerequisite: MEA

This course presents the Office of Management and Budget (OMB) policies, guidance, and strategies for the development and implementation of enterprise architecture, with particular focus upon their application by civil departments and agencies. After a review of the Federal Enterprise Assessment Framework, students examine in greater detail the Federal Segment Architecture Methodology (FSAM), first introduced in the Modeling for Enterprise Architecture course, and associated work-products, as well as their relationships to the enterprise architecture segment reporting requirement templates. Student attention then turns to the Federal Enterprise Architecture reference models and profiles and how they support the development of enterprise architecture and the business case (i.e., OMB Exhibit 300). Next, students explore OMB's direction on Service Oriented Architecture, and cross-cutting organizational initiatives through the Federal Transition Framework. The course concludes with an overview of the Department of Defense (DOD) Architecture Framework to provide insight into DOD's approach for the development of enterprise architecture.

Learning Outcomes: Students will be able to assess the degree to which an agency's enterprise architecture is consistent with the Federal Enterprise Architecture Segment Methodology and recommend appropriate development, implementation, sustainment, or governance strategies. Students will be able to articulate and plan for the dependent relationships between the assessment framework, the segment reporting templates, and the segment methodology to meet OMB enterprise architecture reporting requirements.

FFR—The Future of Financial Reporting and Standards (6602) **Designed for students in the CFO Leadership Certificate.**

This course focuses on the changing directions of financial and management reporting for Chief Financial Officers in a dynamic environment. In response to changing citizen and shareholder expectations, financial statement reporting, budgetary reporting, and cash reporting must be accurate, transparent, and account-

able, and result in "clean" audit opinions. These new reporting expectations and changing accounting standards, require new relationships among federal, state, and local governments, and government contractors, as well as enhanced reporting to internal constituents of the CFO, including program managers and the organizational head. Successful reporting can be facilitated by enterprise architecture, financial systems, and data management techniques.

Learning Outcomes: Students will be able to analyze the changing roles, requirements, and expectations for financial, budget, and program reporting in government organizations from legal, policy, and technological perspectives, to evaluate the enterprise architecture, financial systems and processes, and data management systems that support new reporting challenges, and to design a leadership plan for their organization that responds to current and future reporting expectations for transparency and accountability.

GBE—Government Business Enterprise Transformation (6501)

This course focuses on initiatives, strategies, and opportunities for transforming the Federal Government's business operations that provide capabilities, resources, and materiel to the government employee. The course assesses the structural, political, technological, leadership, and human challenges of effecting transformational change in a complex enterprise. This includes analyzing the challenges transformation initiatives bring when engaging in new ways of doing business, retiring legacy systems, processes, and strategies, while simultaneously delivering required services and results. The evolving vision and development of the Federal Enterprise Architecture as the information technology enabler of business enterprise transformation are evaluated. Students examine large organization transformations from the corporate sector to identify insightful lessons that can be developed as recommendations for government business enterprise transformation.

Learning Outcomes: Students will be able to identify the central dynamics and enablers of initiatives, opportunities, and strategies for transforming the Federal Government's business enterprise; to evaluate and compare transformation efforts across multiple agencies by identifying areas of strengths, weaknesses, and opportunities; and to recommend strategies for addressing them.

GEN—Global Enterprise Networking and Telecommunications (6205)

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

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

GLS—Global Strategic Landscape (6213)

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

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

HST—Homeland Security Information Management: Tools and Techniques (6503)

This course examines information management concepts and issues related to critical homeland security mission areas, including intelligence and warning, border and transportation security, domestic counterterrorism, critical infrastructure protection, catastrophic terrorism defense, and emergency preparedness and response. The course exposes students to tools and techniques that support the planning, mitigation, response, recovery, and prediction aspects as well as crisis and emergency management of homeland security. It explores state-of-the-art and emerging concepts relating to intelligent agents, decision support, data/text mining, visualization, geographical information systems, and computer modeling and simulation.

Learning Outcomes: Students will be able to evaluate prospective homeland security tools and techniques in terms of meeting organizational goals and requirements, and create an implementation strategy for infusing these technologies into their organizations.

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

Prerequisite: Secret Clearance is required.

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

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

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 also explores the role of oversight in the management and leadership of Federal IT acquisition programs.

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

ITA—Strategic Information Technology Acquisition (6415)

This course examines the role senior leaders play in the successful acquisition of information services and technologies to achieve organizational strategic objectives. It employs a life cycle management approach through exploration of statutory and regulatory policies, acquisition strategies, requirements management, analysis of alternatives, design and performance measurement issues, and implementation and sustainment considerations that directly impact IT acquisition. Acquisition best practices are considered, as well as numerous acquisition issues, including Share-in-Savings, Performance-Based Contracting, modular contracting, the broadened availability of commercial items, the use of more flexible selection procedures and procurement vehicles, and contract administration. The course includes guest speakers from government and industry with the latest in policy updates and how to maximize productivity in the contractor government acquisition environment.

Learning Outcomes: Students will be able to analyze agency information technology strategies, methods, and plans, and recommend changes to increase the likelihood that acquisition will fully meet agency mission objectives.

ITP—Information Technology Project Management (6416)

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

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

Course Descriptions

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). The course also examines 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. A lesson on strategic legal implications and considerations is also presented, and an in class exercise examines the use/misuse of IO strategies against an adaptive adversary. The course concludes with a snapshot of current U.S. military IO strategies.

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

LCW—Leading the 21st Century Workforce (6506)

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

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

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 also explores the role of information and technology in the Information Age organization; the relationships among learning, change, and strategic planning; and the new abilities required for leading in the Information Age.

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

LSI—Strategies for Leading Change and Innovation (6511)

This course focuses on the strategies that leaders require to create, implement, and guide their organizations successfully through change and innovation – both that of their own making and that which is driven by external and uncontrollable circumstances. The course examines the drivers of change and innovation to include emerging technologies, globalization, and demographic shifts. It explores models of change and innovation as well as evolving concepts of organizational strategy designed to cope with uncertainty and rapid rates of change. It also examines the barriers to and levers of change and innovation such as leadership, organizational culture, and bureaucratic politics.

Learning Outcomes: Students will be able to develop effective strategies for leading organizations through change and innovation; to analyze the strengths and weaknesses of various strategies; and to leverage organizational culture and bureaucratic politics to achieve successful organizational transformation.

MAC—Multi-Agency Information-Enabled Collaboration (6512)

This course focuses on strategies, means, and information models needed for effective multi-agency collaboration in planning, decision-making and implementation of national security operations, including stabilization and reconstruction, and homeland security and national preparedness operations. It examines current and proposed initiatives for transforming and leading cross-boundary collaboration at the Federal, State and local levels, and includes multilateral collaboration situations with nongovernment (NGO) and international organizations and coalitions, media, private sector and coalition partners. The course examines how information-enabled networks, collaborative tool-sets, cross-boundary information-sharing, and work processes can be harnessed to enable effective multi-agency and multilateral national and homeland security activities. The course assesses the human, social and leadership issues of sustained and effective multi-agency collaborations. Impediments such as legal and budgetary authority restrictions, educational and cultural factors that inhibit cross-boundary mission effectiveness and transformation are assessed, as are strategies for addressing them.

Learning Outcomes: Students will be able to evaluate the principles and dynamics of effective collaboration across agency boundaries and the leader competencies, information technologies and organizational innovations that offer opportunities to enable effective multi-agency collaboration; appraise critically the ends, ways, and means for achieving effective multi-agency collaboration; and formulate and shape transformation initiatives to significantly advance effectiveness in complex operations requiring multi-agency collaboration.

MEA—Modeling for Enterprise Architecture (6439)

Prerequisite: Must be able to install and use an EA modeling repository tool on a non-IRM College computer.

This course explores the use and effectiveness of architectural modeling to describe an organization and examines model-based products as tools to support, influence, and enable organization planning, and decision-making. Hands-on exercises provide students with practical experience with work-products common to the DOD Architecture Framework (DODAF) and Federal Segment Architecture Methodology (FSAM), as well as other established frameworks. A case-study approach focuses on object-oriented models, e.g., Unified Modeling Language (UML) covering process, data, and systems. Structured models, e.g. IDEF, are also examined. Emphasis is placed on the efficacy of modeling styles and

the interpretation of the descriptive models as well as interpreting case-study documentation. Students use an automated modeling tool to develop the descriptive models and to demonstrate the utility of an Enterprise Architecture repository.

Learning Outcomes: Students will be able to interpret both object-oriented and structured-based diagrams and to evaluate the primary characteristics of a model in order to critically assess its quality and the information being depicted.

MOP—Measuring Results of Organizational Performance (6316)

This course focuses on strategic planning and performance in public organizations. It examines planning and performance measurement requirements of current legislation. It provides strategies and techniques for measuring performance and assessing results as part of a strategic planning/budgeting process. The course uses Kaplan and Norton's Balanced Scorecard as a framework to develop leading and lagging measures that link to organizational mission, vision, goals, objectives, initiatives, strategy and outcomes.

Learning Outcomes: Students will be able to develop and/or assess a comprehensive plan for conducting a performance assessment in their organization that directly supports senior decision makers in achieving mission effectiveness.

OCL—Organizational Culture for Strategic Leaders (6321)

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

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

PFM—Capital Planning and Portfolio Management (6315)

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

Learning Outcomes: Students will be able to evaluate an investment portfolio and the corresponding capital planning and invest-

ment management process to ensure that they comply with current statutes and regulations, recommend changes to the process, and develop a strategy for balancing a portfolio of investment projects.

PMA—Planning and Managing Enterprise Architecture Programs (6432) Prerequisite: Successful completion of Architect (Level 1) Certificate.

This course prepares students to lead and manage the planning, development, and implementation of an enterprise architecture (EA) program. It examines critical success factors for initiating an EA program including obtaining and keeping organizational commitment, building effective government-contractor teams, and selecting appropriate tools. Next, students explore topics necessary to conduct an EA program, including establishing EA scope and level of detail; adapting a selected EA methodology to address real-world time and budget constraints, and evaluating and managing risk. With this foundation, students plan appropriate EA program management strategies in response to case-study scenarios.

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

PRI—Strategies for Process Improvement (6333)

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

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

RIA—Leadership for Risk Management, Internal Controls, and Auditing (6603)

This course, designed for students in the CFO Leadership Certificate, examines how effective leadership by CFOs in assessing risk, managing internal controls, and audit management can lead to enhanced efficiency, effectiveness, and transparency of an organization. The course also examines the influence of internal control, federal risk management, and auditing requirements on federal, state, and local governments.

Learning Outcomes: Students will be able to analyze factors that contribute to effective risk management, internal controls and auditing, evaluate the relationships between financial leaders and auditors in terms of roles and processes and to design an effective risk management and internal controls system for planning, executing, and coordinating a government organization's functions.

Course Descriptions

SAL—Software Acquisition Leadership (6410)

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

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

SCL—Strategic Communication for Government Leaders (6322)

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

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

SCS—Managing Security of Control Systems (6210)

This course explores a wide range of people, processes, and technology issues in the management of critical infrastructure control systems (CS) security including Supervisory Control and Data Acquisition (SCADA) systems security. Systems for monitoring and controlling base-level and regional supply and flow of resources such as electricity, lighting, water, gas, and transportation are examined. Topics include CS components, threats, and vulnerability assessment and technical measures for improving security unique to CS, such as multifactor authentication, telephony firewalls and radio frequency encryption, and operational and physical security. The CS industry and initiatives in CS security standards are explored. This includes a focus on the interplay between regional commercial providers and baselevel continuity of operations. The move toward integration of CS with traditional computer networks is covered.

Learning Outcomes: Students will be able to assess a control systems environment for people, processes, and technology vulnerabilities, and recommend an improved security strategy.

SEC—Cyber Security for Information Leaders (6201)

This course explores concepts and practices of defending the modern net-centric computer and communications environment. The course covers the 10 domains of the Certified Information System Security Professional (CISSP®) Common Body of Knowledge

(CBK®). In addition, the course covers a wide range of technical issues and current topics including basics of network security; threats, vulnerabilities, and risks; network vulnerability assessment; firewalls and intrusion detection; transmission security and TEMPEST; operating system security; web security; encryption and key management; physical and personnel security; incident handling and forensics; authentication, access control, and biometrics; wireless security; virtual/3D Worlds; and emerging network security technologies such as radio frequency identification (RFID) and supervisory control and data acquisition (SCADA) security. The course also defines the role of all personnel in promoting security awareness.

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

SIO—Strategic Infrastructure Operations (6214)

This course is TS/SCI and is limited to U.S. citizens. It can only be taken through the NDU elective program or by M.S. Degree IO Concentration students.

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.

Learning Outcomes: Students will be able to analyze the national security impact of society's dependence on interconnected critical infrastructures and to develop effective strategies to protect those fragile critical infrastructures.

SPA—Privacy Rights and Identity Management in the Information Age (6508)

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

Learning Outcomes: Students will be able to (1) recommend appropriate protection strategies, tools, and methods for processing and sharing private information, and (2) develop policies to manage privacy in government initiatives.

STA—Solutions Architecture and Transition Planning for Architecture (6440) Prerequisite: Successful completion of Level II courses. Students will be required to install a required EA modeling repository tool on a non-IRM College computer.

This course prepares the senior or chief architect to collaborate

with the solutions architect(s) to develop target enterprise-wide technology architecture and solution strategies that complement and enable the target enterprise business environment. Students examine a general target technology framework and explore alternative technology architecture end-states for enterprise-wide service oriented architecture and capabilities-based architecture. For each general design end-state, alternative criteria are considered to provide alternative technical designs. In addition, approaches to harmonizing target segment solution architectures with the enterprise target technology architecture are explored. Students examine strategies for developing a security architecture to include the Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP). The course concludes with a consideration of alternative legacy migration and transition strategies. These techniques and strategies will be explored through case studies using automated EA and support decision tools to provide critical hands-on experience.

Learning Outcomes: Students will be able to design macro-level target technology architectures and develop alternative transition plans as a function of target end-state. (This course won't be offered until the 2010-2011 academic year.)

TAS—Transformation as a Strategic Alignment (6528)

This course explores the fundamental nature and dynamics of transformation, and the disequilibrium and ambiguity surrounding the search for and transformation of new mission spaces. It investigates those perilous but essential changes that allow an organization to create new organizational capabilities, exploit technologies, and take advantage of performance possibilities to achieve new levels of mission effectiveness or move into new mission spaces. This course examines the nature and interdependencies of the turbulent, globalized, and technologically catalyzed and infused environment in which traditional organizational interventions are increasingly inadequate. It analyzes the need for and type of new governance that can and will lead the transformation effort that results in the critical strategic alignment underpinning of agile, responsive, and relevant organizations and mission capabilities.

Learning Outcomes: Students will be able to analyze the global economic, social, and technological forces catalyzing transformation efforts; assess how this strategic landscape drives and shapes transformation opportunities and possibilities in their own and other government organizations; and create, evaluate, and recommend an appropriate governance structure that allows for an effective and sustained transformation.

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 also provides a risk management framework to help information leaders leverage the benefits of Internet technologies while minimizing the risks that such technologies pose to their organizations.

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

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

This course explores the capabilities, selection and strategic 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., semantic computing, cloud computing, web services, social networking, geographic information services technology, media-centricity, and security. It concludes with a consideration of web technology evaluation criteria, methodologies, and risks.

Learning Outcomes: Students will be able to evaluate the benefits and risks of current and emerging web technologies and their strategic advantages and disadvantages to accomplish their agency's mission.



Academic Partners

The IRM College forms academic partnerships with universities and colleges across the United States. Graduates from the college's certificate programs can apply to a number of partner institutions for completion of a Master's or Doctoral Degree. Academic partners accept 9, 12, or 15 graduate semester credits depending on which certificate program was completed at the IRM College. Many academic partners provide full-time, part-time, and online educational opportunities.

As of catalog print date, there are 39 current IRM College academic partners, and their degree programs (as covered by the Memoranda of Understanding, MOU) are listed below. Please refer to the IRM College website partnership matrix (http://www.ndu.edu/irmc/ntwk_list1.htm) for more details on the exact number of credits and points of contact at each partner institution. The college anticipates that some partner schools will be adding the IRM College's newest certificate programs, Chief Financial Officer (CFO) and Government Strategic Leader (GSL), to their MOUs in the coming year. Please check the website often for changes and additions.

Questions about the partnership program should be directed to Patty Coopersmith, IRM College Academic Partnership Coordinator, at coopersmithp@ndu.edu, 202-685-2117. Specific questions about degree programs, admission requirements, or remaining courses should be directed to the academic partner institution representative.



Dr. Brenda Roth (center) and Patty Coopersmith (2nd from right) attend a signing ceremony to renew the Memorandum of Understanding with Capitol College. From Capitol College are Dr. Michael Wood (second from left), President of Capitol College, Dr. Vic Maconachy (left), VP for Academic Affairs, and Ken Crockett (right).

Current IRM College Academic Partners

Air Force Institute of Technology (OH)

Auburn (AL)

Capitol College (MD)

Central Michigan University (MI)

Clemson University (SC)

Drexel University (PA)

East Carolina University (NC)

Eastern Michigan University (MI)

Florida Institute of Technology (FL)

George Mason University (VA)

James Madison University (VA)

Johns Hopkins University (MD)

Missouri University of Science & Technology (MO)

Mississippi State University (MS)

New Jersey City University (NJ)

New Mexico Tech (NM)

Northeastern University (MA)

Norwich (VT)

Pace University (NY)

Polytechnic University (NY)

Regis University (CO)

Rochester Institute of Technology (NY)

San Diego State University (CA)

Syracuse University (NY and DC)

Texas A&M (TX)

Towson University (MD)

University of Dallas (TX)

University of Detroit Mercy (MI)

The University of Illinois at Urbana Champaign (IL)

University of Maryland Baltimore County (MD)

University of Maryland University College (MD)

University of Nebraska at Omaha (NE)

University of North Carolina at Charlotte (NC)

University of Pittsburgh (PA)

University of Texas at San Antonio (TX)

University of Tulsa (OK)

University of Washington (WA)

Virginia Tech (VA)

Walsh College (MI)

Student Services and Policies

Admission

IRM College courses are available to Federal civilian government employees, military officers, and non-Federal Government employees (such as State and local government employees, and private sector employees sponsored by a government agency).

To register for a course, a prospective student must first be admitted to one or more IRM College programs. The IRM College is solely responsible for determining its admission criteria and for determining which applicants are admitted.

Eligibility Criteria

See table below.

Change in Eligibility: The College will periodically review eligibility of active students. If a student's eligibility changes (employer, pay grade, rank, etc.), he or she must notify the College. 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 owed.

International Students: International students (non-U.S. citizens) must apply through the appropriate Security Assistance Training Field Activity (SATFA) country program manager.

Program completion time limit:

Certificate programs: All coursework applied toward a certificate must be completed within four years.

Master of Science (M.S.) Degree program: All coursework applied toward a M.S. Degree must be completed within the previous seven years.

Students must successfully complete at least one course every 18 months to maintain active status in a program.



CONTACT INFORMATION:

Office of the Registrar:

IRMRegistrar@ndu.edu

Tel: 202-685-6300

DSN: 325-6300

Fax: 202-685-4860

IRM College
300 5th Ave., Bldg 62
Marshall Hall
Washington, D.C. 20319

Eligibility Criteria	
1. U.S. Government Affiliation.	Federal civilian government employees, military officers, and non-Federal Government employees (such as State and local government employees, and private sector employees sponsored by a government agency). Private sector employees are not eligible to enroll in the M.S. degree program.
2. Education	All students must possess a Bachelor's Degree from a regionally accredited U.S. institution or the equivalent from a foreign institution. <i>Additional for M.S. Degree Program: The minimum grade point average (G.P.A.) is 3.0 on a 4.0 scale (a "B" grade average) for all previous undergraduate and graduate work. In cases where the undergraduate G.P.A. is below a 3.0, the G.P.A. for the last two years will be used to determine eligibility.</i>
3. Pay Grade/Rank, Experience	Various, by Program
<i>Advanced Management Program (AMP)</i>	Federal civil service pay grade of GS/GM-13 or equivalent / military officer rank of O-5.
<i>Certificate Programs (non-AMP, CFO; includes PD)</i>	Federal civil service pay grade of GS/GM-12 or equivalent / military officer rank of O-4.
<i>CFO Leadership Certificate Program (CFO)</i>	Federal civil service pay grade of GS/GM-14 or equivalent / military officer rank of O-5. Experience: Three years of federal financial management experience is required. Documented Knowledge of Financial Management: Undergraduate or Graduate degree in finance or business field, CPA, CGFM or CDFM.)
<i>Masters of Science (M.S.)</i>	Federal civil service pay grade of GS/GM-12 or equivalent / military officer rank of O-4.

"Best team of Instructors I've ever had the pleasure of interfacing with. They all had expert knowledge of their subject areas and a willingness to share personal experience to facilitate our learning. This greatly encourages the pursuit of excellence. Thanks a Million!"

Required Documents for AMP and Certificate Programs

Detailed application instructions, forms and templates are available online.

Advanced Management Program (AMP)

- Application for Admission
- Résumé
- Nomination Letter

Certificate Programs (non-AMP, CFO; includes Professional Development)

- Application for Admission
- Employer Verification and Sponsorship Form
- Private sector only: Résumé

CFO Leadership Certificate Program (CFO)

- Application for Admission
- Employer Verification Form for the CFO Leadership Program
- Private sector only: Résumé

Required Documents for M.S. Program

- Application for Admission
- Résumé
- Employer Verification Form for the GSL Master of Science Program
- Recommendations (2)
- Official Transcript(s)
- Statement of Purpose

1. Résumé. The résumé should include a work history that describes the applicant's position title, organization, responsibilities, and accomplishments, and any awards or recognitions earned. If there are gaps in the résumé, a short paragraph is needed to explain them.

2. Employer Verification Form for the GSL Master of Science Program (M.S.-EV Form). The Employer Verification Form is used to verify employment. A template can be found on the IRM College website at http://www.ndu.edu/irmc/admis_appover5.htm. The applicant may also attach additional comments in support of his/her application.

The applicant's most immediate supervisor or Human Resources Officer holding a grade of GS/GM-12, O-4, or higher, must complete and submit the form, printed on organizational letterhead, directly to the IRM College (fax: 202-685-4860 or scanned attachment to IRMCRRegistrar@ndu.edu).

3. Recommendations (2). Two recommendations are required for admission to the M.S. Degree Program. Recommendations should be completed on either

the Recommendation form provided on the IRM College website (http://www.ndu.edu/irmc/admis_appover5.htm) or on organizational letterhead. All recommendations, regardless of format must address the questions which are asked on the form. At least one recommendation must come from an individual in the applicant's professional supervisory chain. The second may come from another professional source or from a faculty member who has taught, or otherwise, academically assessed the applicant. Both recommendations should be written by persons able to judge the applicant's ability to complete a challenging graduate-level degree program.

Recommenders are asked to comment on the applicant's leadership potential, academic ability, motivation to complete the degree program, and the applicant's commitment to leading Information Age defense and government organizations. Recommendations must be sent directly from the nominator via fax or scanned attachment to IRMCRRegistrar@ndu.edu. Recommendation forms (or letters) emailed directly from the student will not be deemed official.

4. Official Transcript. Applicants must submit one official transcript from the 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) is 3.0 on a 4.0 scale (a "B" grade average) for all previous undergraduate and graduate work. In cases where the undergraduate GPA is below a 3.0, the GPA for the last two years may be used to determine eligibility.

An official transcript bears the official seal of the issuing institution. Please request that official transcripts be sent to the Registrar's Office at IRM College Registrar, 300 5th Avenue, Bldg 62, Fort McNair, DC, 20319. Photocopies, while not considered official, may be submitted to expedite the processing of applications. Transcript requests for academic work completed at the National Defense University need not be submitted.

5. Statement of Purpose. The statement of purpose is a 250-500 word essay that addresses the applicant's reason for undertaking the program, goals, experiences, and expected results. In this statement, applicants should directly discuss their leadership potential, academic ability, and motivation to complete the degree program successfully in a timely manner. Applicants should also discuss their level of commitment to leading Information Age defense and government organizations.

The M.S. Degree is a selective and competitive degree program.

Admit Status

Applicants approved for admission by the College leadership will be placed into one of three admission categories.

Regular Admission: Applicants who meet all eligibility criteria are awarded regular admission.

Probationary Admission: Applicants who fail to meet one or more of the requirements for regular admission may be admitted on probation, provided additional evidence of capacity to do satisfactory work is presented. Students entering on probation will remain on probation until the successful completion of two courses.

Provisional Admission: Provisional admission may be considered for applicants who appear to be admissible on the basis of the credentials submitted, but who are unable to supply all of the required official records prior to registration. Students admitted provisionally must submit complete and satisfactory records within 60 days of the acceptance date. If these credentials are not received by the date specified or if they prove to be unsatisfactory, the student will not be permitted to register for future courses. Provisional admission does not guarantee subsequent regular admission.

Course Registration

Students who are in the Advanced Management Program (AMP) will automatically be enrolled in the courses necessary for completion of the program. Students in the Master of Science Degree program, the certificate programs, or the Professional Development program must self-enroll in the desired courses using the College's online student information system.

Enrollment Procedures

The IRM College will assign the student an account, Username, and Password that he or she will use to self-enroll in classes (link from www.ndu.edu/irmc) once accepted into a program. (Detailed instructions are sent at time of admission.)

Confirmation of Enrollment

Students may confirm successful enrollment by viewing their course schedule online. A course acceptance notice will automatically be sent to students who successfully enroll in a course. The IRM College may send additional reminders and attendance confirmation requests prior to the course start date.

Pre-course Materials and Assignments

Each course has readings and other pre-course activities that allow students to prepare for the first day of their course. Pre-course materials will be posted to the IRM College's eLearning system (Blackboard) no earlier than 13 days before the start of class.

No Show Policy

The College will assign students who do not disenroll (via the online registration system, the Registrar's Office, or the Offering Leader) by the start date an enrollment action of "No Show" (NS). Students will be prohibited from taking courses for six months if they receive two or more NS notices.

Fees

There are no fees for DOD employees for IRM College courses or academic programs. This includes all course offerings and the Advanced Management Program, but may not include special offerings such as executive or special seminars.

Note: Military members in the Reserves or National Guard must be in active duty status at the time the course is in session and present orders to receive the DOD tuition waiver. If not presented, the student will be liable for the full tuition owed.

FY10: The FY 2010 intensive course fee for non-DOD Federal, State, and local government employees is \$1,100. The FY 2010 intensive course fee for private industry students is \$1,995.

The Advanced Management Program (AMP) fee for non-DOD Federal, State, and local government employees for FY10 is \$10,500. The fee for private industry students is \$16,500.

Payment Instructions

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

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

Program Completion

Program certificates are prepared annually for the IRM College's graduation exercise. The College holds the annual commencement exercise in April, and those who complete programs throughout the year are eligible to attend. Ceremonial certificates are mailed to the home address of students who do not attend the ceremony. Students are responsible for maintaining mailing and shipping addresses in uNET to ensure delivery is not delayed.

The IRM College Graduation Exercise for Academic Year 2010 is tentatively scheduled for April 30, 2010 (check the IRM College website for exact date and time). The Registrar will contact all known and potential graduates at the students' preferred e-mail address as shown in uNET approximately eight weeks prior to graduation. This e-mail message will provide detailed timelines and procedures that students must follow to be included in graduation planning.

Students who are attempting to complete their programs within two months prior to graduation exercises in April are advised to work closely with their advisor and course instructors to ensure they meet requirements in time for graduation. Students may use the program requirements of the catalog in force at the time of his or her initial acceptance, or the student may choose to fulfill the requirements of the current catalog.

Completion Procedures

Students of the IRM College who have completed certificate program requirements must compete and return an "Application for Graduation" by email directly to the IRM College. (Exception: Candidates for a Master of Science Degree should consult the M.S. Program academic advisor regarding graduation procedures.)

To officially graduate the program, the student must:

1. Be admitted in the academic program(s) he or she intends to complete.
2. Complete all course requirements. (The student may use the program requirements of the catalog in force at the time of his or her initial acceptance, or the student may choose to fulfill the requirements of the current catalog.)
3. Verify final grades are accurate (view unofficial transcript). (A passing grade for all applicable certificate 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.)

4. Complete and submit the "Application for Graduation" form.

Upon approval of the academic dean, the certificate name and completion date will be noted on the student's official transcript and the Registrar's Office will send a 'program completion letter' signed by the Senior Director to the student's home address on record.

The date noted in the program completion letter or official transcript is the official completion date. Dates on certificates awarded at the College's graduation ceremony reflect the ceremony date and should not be used for reporting purposes.

Records Maintenance

The IRM College maintains hard copy and electronic records as required for all prospective, current, and past students. Current students are responsible for ensuring their current biographic and demographic information is correct in uNET to assist the IRM College in meeting Federal and Department of Defense directives and reporting requirements.

Transcripts

Two types of transcripts are available from the IRM College.

Unofficial Transcripts. Students with an account in uNET can print unofficial transcripts from their uNET account at any time.

Official Transcripts. Students may request official transcripts by sending a signed request that includes the student's full name, Social Security number, and phone number and address of the transcript recipient. Requests should be faxed to the Registrar's Office at 202-685-4860 or DSN 325-4860. Official transcripts are produced and mailed weekly. Official transcripts are printed on copy-safe National Defense University transcript stock, bear the University's raised seal, and are signed by the University Registrar. Reproductions are clearly marked as copies and are not considered official.

Academic Policies

General Policies

Admission to Multiple Academic Programs

Students may apply for and be admitted to more than one IRM College academic program at a time.

Program Completion Time Limit

Certificate programs: All coursework applied toward a certificate must be completed within the four years before the termination of the program.

Master of Science (M.S.) Degree program: All coursework applied toward a M.S. Degree must be completed within the previous seven years.

Students must successfully complete at least one course every 18 months to maintain active status in the program.

Applying Coursework Earned Prior to Program Admission

Certificate Program Participants. If a participant has completed IRM College coursework under another program, he or she may apply eligible courses to another certificate program. Eligible courses are those that meet a program's requirements. Courses taken for a grade of Audit (AU) or Professional Development (PD) are not applicable. All coursework applied toward a certificate must be completed within the previous four years.

Masters of Science Program Participants. If a participant has completed IRM College coursework under another program, he or she may apply eligible courses to the Master of Science Degree program. Eligible courses are those that directly apply to the Master of Science Degree requirements. Courses taken for a grade of Audit (AU) or Professional Development (PD) are not eligible. All coursework applied toward a M.S. degree must be completed within the previous seven years.

Program Actions

Drop. The IRM College may drop students from a certificate program for a number of reasons that include, but are not limited to, failure to successfully complete a course within an 18-month period or earning multiple grades of "No Credit."

Withdrawal. Students who wish to end their participation in an IRM College certificate program may submit a written request to the Registrar. 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 may be e-mailed to IRMCRegistrar@ndu.edu. Confirmation of withdrawal will be provided by e-mail.

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

Dismissed. Students may be dismissed from academic program(s) upon the decision of the Academic Review Board.

Requirements for Continued Enrollment

Students enrolled at the IRM College must maintain satisfactory progress. Students are expected to achieve a satisfactory grade (A, A-, B+, B) in all coursework attempted for graduate/certificate credit.

An accumulation of two grades of NC or W will result in suspension of the student's enrollment. A student whose enrollment has been suspended because of unsatisfactory grades is ineligible to register until properly reinstated by approval of the Dean.

A student reinstated will be placed on probationary status and expected to complete all future coursework with satisfactory performance. Should the student receive a grade of NC or W after being reinstated in the program, his or her enrollment in the college will be terminated.

Academic Policies



CONTACT INFORMATION:

Office of the Registrar:

IRMCRegistrar@ndu.edu

Tel: 202-685-6300

DSN: 325-6300

Fax: 202-685-4860

IRM College

300 5th Ave., Bldg 62

Marshall Hall

Washington, D.C. 20319

"I have grown tremendously, both personally and professionally, from my coursework at the IRM College. Although I am graduating from the CIO Program soon, I will enroll in another program and continue my education. The IRM College is one of the great educational benefits for the government employee."

Grading

The IRM College's grading system follows:

- A** Work of exceptional quality at the executive/graduate level.
- A-** Work of very high quality at the executive/graduate level.
- B+** Work of high quality at the executive/graduate level.
- B** Work of acceptable quality at the executive/graduate level.

No Credit (NC): When an "NC" grade is assigned, the student will not receive academic credit for the class.

This grade is used when:

- Attendance/participation requirements are not met.
- Academic requirements are not submitted on time (original due date with no written request for an extension, or extension granted but requirements not submitted by new due date).

Students enrolled in Distributed Learning (DL) courses do not participate by the end of the third week and are dropped by the faculty Offering Leader.

Students withdraw after 25 percent of the course has been taught (e-resident or DL).

Students do not meet academic requirements on resubmission of an unacceptable academic requirement.

Incomplete (I): This grade is assigned to a student who:

Is granted an extension to submit the academic requirements (usually a final paper and/or project). If a student needs an extension, he or she must request it in writing to the Offering Leader for the class prior to the assignment deadline. The written request must provide acceptable reasons for an extension and a proposed deadline for submission. Approved extensions are typically for two to three weeks.

Submits the academic requirement on time but receives a grade below a "B" and the student subsequently resubmits his or her work. The Offering Leader may grant the student two to three weeks to resubmit the academic requirement.

In either case, if a student receives an approved extension to submit academic requirements, the highest possible final grade the student can obtain is a B+. If a

student submits a final assessment under an extension that does not meet academic requirements but the student satisfactorily met the attendance/participation requirements for the course, the Offering Leader may assign a PD.

Note: Students wishing an additional extension past the original extension granted by the Offering Leader may submit a request with proper justification to IRMCEXceptionRequest@ndu.edu

Withdraw (W): When the student requests withdrawal from a course after the start date but within the first 25 percent of the course, the faculty member will assign a grade of "W." The request to withdraw must be submitted in writing to the Offering Leader. If the student requests withdrawal after 25 percent of the course is completed, the faculty member will assign a grade of "No Credit."

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

Audit (AU): Beginning in AY 2006/2007, the Audit (AU) grade is no longer used. However, students who audited courses prior to AY 2006/2007 will have an AU grade posted to their official transcripts.

Other Annotations:

No Show (NS): The student did not report for a scheduled class. An "NS" annotation does not become part of a student's official transcript, but a student receiving two grades of NS will be prohibited from enrolling for six months.

Academic Integrity

The College has a zero tolerance policy toward plagiarism and other forms of cheating. All requirements submitted by students must be their original work, produced for the first time while they are at the IRM College. The product should contain the student's own ideas and analysis except as documented by appropriate citations, and must be submitted for academic credit only once to satisfy course requirements.

Plagiarism is the unauthorized use, intentional or unintentional, 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. Students are encouraged to submit their papers and assessments through the plagiarism detection software, "SafeAssignment," found in the Student Center Portal in Blackboard prior to turning them in for grading.

Submission of false admission eligibility credentials or violations of the academic integrity policy are referred to the Academic Review Board. Sanctions range from expulsion, suspension, revocation of certificates, a grade of No Credit, rejection of the work submitted for credit, or a letter of admonishment. The authority for decisions and actions rests at the College.

Negative academic actions may be disclosed to the student's sponsoring service or organization, as well as to investigators for employment or security clearances.

Academic Review Board

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

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

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

Student Assessment

All IRM College students must demonstrate a successful level of mastery of the intended learning outcomes of each course. The faculty 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 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 IRM College, 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).



A group of international officers attend a class in the Cybersecurity Laboratory.

Faculty & Administration

Leadership

ROBERT D. CHILDS, Senior Director; B.S., Grove City College; M.A.T., Duke University; Ed.D, University of Denver; Air Command and Staff College; National War College, National Defense University; Fuqua Business School, Duke University.

ELIZABETH A. McDANIEL, Dean of Faculty and Academic Programs; B.A., University of Florida; M.A., Barry University; Ph.D., University of Miami.

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

BRENDA F. ROTH, Assistant Dean for Curriculum; B.A., University of Arizona; M.Ed., University of South Carolina; M.A., University of Colorado at Boulder; Ph.D., University of Virginia.

PAULETTE ROBINSON, Assistant Dean for Teaching, Learning, and Technology; B.A., University of Hawaii; M.A., University of Hawaii; M.N.A., University of San Francisco; Ph.D., University of Maryland.

MARY S. McCULLY, Chair, Information Strategies Department; 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.

GILLIAM E. DUVALL, Chair, Information Operations and Assurance Department; B.S., Purdue University; M.S., The Naval Postgraduate School.

ANDREW (ANDY) P. GRAVATT, Chair, Systems and Technology Department; B.S., University of Maryland; M.S., The Johns Hopkins University Whiting School of Engineering.

PATRICIA COOPERSMITH, Project Manager of Educational Initiatives; B.S., The Pennsylvania State University; M.B.A., Augusta State University.

DONNA POWERS, Lieutenant Colonel, USAF, Director of Operations; B.S., University of Washington; M.A., Golden Gate University.

CASSANDRA LEWIS, Project Manager of Academic and Faculty Enhancement; B.A., University at Buffalo; M.A., Boston College; Ph.D., University of Maryland.

Faculty

RICARDO AGUILERA, DOD Comptroller Chair, Chief Financial Officer Academy; B.A., New York University; M.A., The George Washington University.

JAY ALDEN, Information Strategies Department; B.S., Long Island University; M.S., Hofstra University; Ph.D., Hofstra University.

NATE ALLEN, Lieutenant Colonel, USA, Information Strategies Department ; B.S., United States Military Academy ; M.A., University of Colorado ; M.B.A., University of Colorado ; Ph.D., George Washington University.

WILLIAM BODDIE, Systems and Technology Department; B.A., Saint Leo College; M.A., Webster University; M.S., George Mason University; Ph.D., The University of Phoenix.

MARY COLE CARROLL, Information Operations and Assurance Department; B.A., Metropolitan State College of Denver; M.B.A., The George Washington University; M.S., Industrial College of the Armed Forces, National Defense University; J.D., Georgetown University Law Center.

JOHN T. CHRISTIAN, Information Strategies Department; B.A., University of Virginia; M.A., Ph.D., Vanderbilt University.

JAMES F. CHURBUCK, Information Operations and Assurance Department; B.S., United States Naval Academy; M.S., Industrial College of the Armed Forces, National Defense University.

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

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

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

MARK R. DUKE, Information Operations and Assurance Department; B.A., Sam Houston State University; M.S., George Mason University; M.A., Webster University.

ADRIENNE LATRICE FERGUSON, CFO Academy; B.S., Grambling State University; M.P.A., American University.
PAUL H. FLANAGAN, Systems and Technology Department; A.A., Richard Bland College; B.S., Virginia Commonwealth University; M.A., University of Maryland.

GERRY GINGRICH, Information Strategies Department; B.S., University of North Carolina; M.S., Ph.D., University of Maryland; Post-Doctoral Fellowship, University of Minnesota.

KEVIN T. GRZELKA, Lieutenant Colonel, USA, Systems and Technology Department; B.S., University of Florida; M.S., Florida Institute of Technology, Command and General Staff College.

DENNIS HALL, Systems and Technology Department; B.S. in EE, University of Illinois; M.S. in EE, University of Illinois; M.S.A. in IRM, George Washington University.

TODD HOLMES, CFO Academy; B.S., The Citadel; M.B.A., Golden Gate University; D.A., George Mason University.

CARL (CJ) HORN, Lieutenant Colonel, USA, Information Strategies Department; B.S., United States Military Academy; M.A., Ph.D., The Ohio State University.

MARWAN M. JAMAL, Information Operations and Assurance Department; B.S., M.S., Ph.D., The George Washington University.

JAMES E. KASPRZAK, Information Operations and Assurance Department; B.S., Canisius College; U.S. Army Command and General Staff College; Air War College; Ph.D., Loyola University.

CON KENNY, Systems and Technology Department; B.S., University of Pennsylvania; M.S., George Mason University.

DANIEL T. KUEHL, Information Operations and Assurance Department; B.A., Allegheny College; M.A., Temple University; Ph.D., Duke University.

LUIS G. KUN, Information Operations and Assurance Department; B.S., M.S., Ph.D., University of California, Los Angeles.

IRVING LACHOW, Information Operations and Assurance Department; A.B., B.S., Stanford University; Ph.D., Carnegie Mellon University.

STEPHEN W. MANCINI, Captain, USAF, Information Operations and Assurance Department; B.S., Chapman University; M.S., Air Force Institute of Technology.

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

Faculty & Administration

Faculty (continued)

GARY MAUPIN, CFO Council Faculty Chair, CFO Academy; B.S., George Washington University; M.B.A, George Washington University.

MARK MCGIBBON, Lockheed Martin Visiting Faculty, Systems and Technology Department; B.S., University of Utah; M.S. in ITM, Naval Postgraduate School.; Ph.D., Northcentral University.

TERRY MCGOVERN, Lieutenant Colonel, USAF, Information Strategies Department; B.A. University of Iowa; M.H.S. University of Great Falls; M.S. Air Force Institute of Technology; D.M. University of Phoenix.

ROBERT A. MILLER, Information Operations and Assurance Department; B.A., University of Chicago; Ph.D., Princeton University; J.D., The George Washington University.

EDWARD M. (MATT) NEWMAN, Systems and Technology Department; B.S., University of Maryland; M.S., The American University.

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

ANGELO RIDDICK, Colonel, USA, Information Operations and Assurance Department; A.A., Marion Military Institute; B.A., Albany State University; M.S., National Graduate School.

JOHN R. ROSSI, Information Operations and Assurance Department; B.A., University of Rhode Island; M.A., Rhode Island College.

DANIEL J. RYAN, Information Operations and Assurance Department; B.S., Tulane University; M.A., University of Maryland; M.B.A., California State University; J.D., University of Maryland.

JOHN H. SAUNDERS, Information Operations and Assurance Department; B.S., The Pennsylvania State University; M.B.A., Ph.D., The George Washington University.

KATHLEEN M. SCHULIN, Information Strategies Department; B.A., George Mason University; Industrial College of the Armed Forces; M.P.A., D.P.D.S., University of Southern California.

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

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

VERONICA WENDT, LTC, USA, Systems and Technology Department; B.S., United States Military Academy; M.S., University of Maryland University College.

KAREN WHEELESS, Information Strategies Department; B.A., M.B.A., Baylor University; D.P.A., University of Southern California.

ROBERT E. YOUNG, Information Operations and Assurance Department; B.S., M.S., University of Nebraska Medical Center; D.H.Sc., NOVA Southeastern University.

IRM College Contact Information

WORLD WIDE WEB: <http://www.ndu.edu/irmc>

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

Senior Director	3886
Dean of Students and Administration	3885
Dean of Faculty and Academic Programs	3884
Director, Advanced Management Program	3896

Office of the Registrar **6300**

Fax 4860

E-mail: IRMCRegistrar@ndu.edu

Department Chairs

Information Operations and Assurance Dept.	3889
Information Strategies Dept.	3178
Systems Management Dept.	2069

Faculty and Administrative Fax **3974**

MAILING ADDRESS:

Information Resources Management College

ATTN: Name or Duty Title

Building 62

300 5th Avenue

Fort McNair, Washington, D.C. 20319-5066

2009-2010 Academic Calendar

September 2009	First DL Session Begins
September 8, 2009	AMP 39 International students in-processing and orientation
September 14, 2009	AMP 39 Begins
December 18, 2009	AMP 39 Graduation
January 2010	Second DL Session Begins
January 19, 2010	AMP 40 International students in-processing and orientation
January 25, 2010	AMP 40 Begins
April 30, 2010	AMP 40 and IRM College Graduation
May 2010	Third DL Session Begins
September 7, 2010	AMP 41 International students in-processing and orientation
September 13, 2010	AMP 41 Begins
December 17, 2010	AMP 41 Graduation

INFORMATION RESOURCES MANAGEMENT COLLEGE



CIO



IRM COLLEGE
NATIONAL DEFENSE UNIVERSITY
300 5TH AVE, BLDG 62
FORT MCNAIR, DC 20319
202.685.6300
WWW.NDU.EDU/IRMC



NATIONAL DEFENSE UNIVERSITY