



2006 - 2007
C A T A L O G



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

Director	3886
Dean of Students and Administration	3885
Dean of Faculty and Academic Programs	3884
Director, Advanced Management Program	3896
Registrar	2097

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, D.C. 20319-5066

Catalog is current as of August 1, 2006.
Updates are made on the IRM College website at
www.ndu.edu/irmc.



TABLE OF CONTENTS

IRM College Overview

Mission, Vision, and Goals	4
Message from the Director	5
The IRM College Educational Experience	6
The College at a Glance	8

Programs

Advanced Management Program (AMP)	13
Chief Information Officer (CIO) Certificate	17
Enterprise Architecture (EA) Certificate	19
Information Assurance (IA) Certificates	20
Information Technology Project Management (ITPM) Certificate	22
Organizational Transformation (OT) Certificate	23
General Studies	25

Student Services and Policies

Admissions Policy	27
Eligibility Criteria	27
Application Instructions-Overview	28
General Application Instructions	29
Fees	30
Payment Instructions	31
Course Registration	31
Other Student Services	32
Academic Review Board	33
Academic Advising and Policies	33
Grading	34
Academic Integrity	35
Course Evaluation	36
Instructional Formats	36
Professional Development	36

Course Descriptions	37
----------------------------------	----

Academic Partnership Program	60
---	----

IRM College Faculty	68
----------------------------------	----

MISSION, VISION & GOALS



MISSION

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

VISION

Recognized world leader in information resources management education.



GOALS

- Foster critical thinking and leadership through high-quality graduate-level executive education and research in information resources management to support national security and government effectiveness.
- Continually upgrade curriculum to reflect the changing environment, technological advancements, and evolving stakeholder and customer needs.
- Use state-of-the-art educational and information technology both in the curriculum and in the facilitation of learning.
- Nurture and expand strategic partnerships and interactions with the Department of Defense, private sector, academia, international organizations, and other government agencies to enhance learning opportunities.
- Continually invest in faculty and staff intellectual capital to promote excellence and leadership in IRM education, scholarship, and student learning.
- Leverage information technologies to strengthen college administration, and to enhance educational services and foster lifelong learning in the global IRM, government, and Department of Defense communities.



The IRM College is a global learning community for government's most promising information leaders.

In the Information Age, information technology enables leaders to access information to make faster, better, and more effective decisions. Now, more than ever, the country needs leaders who can effectively develop, organize, manage, and protect the country's various information resources to ensure our national and international security. The IRM College graduate-level certificate programs develop strategic leaders in several critical areas of national security. The College fosters interagency collaboration by providing learning opportunities for individuals who are sponsored by their organizations as promising information leaders. The IRM College, recognized for its academic excellence, partners with over 25 universities and colleges. Graduates from the IRM College's certificate programs can apply up to 15 credits to a partner institution toward completion of a master's or doctoral degree program.

The IRM College's students live and work across the country and the world, including Korea, Iraq, Afghanistan, and Kuwait. By the close of FY 2006, the college offered more than 250 course offerings in the Chief Information Officer, Information Assurance, Organizational Transformation, Acquisition, Enterprise Architecture, IT Project Management, and Information Operations programs—a 17 percent increase over last year. As evidence of the College's global delivery formats, nearly 1,000 students will have completed distributed learning offerings this year from their offices and residences across the country and around the world.

Our challenging programs, offered in residence and over the Internet, meet the needs of a diverse and vital government workforce. Our international and global U.S. faculty understand the challenges, opportunities, policies, and priorities of the U.S. and international government organizations. With their extensive experiences in government agencies, the Department of Defense, the private sector, and higher education, they stay connected and bring the latest innovations and issues from the field.

As a leading graduate- and executive-level DoD institution of higher education, the College continues to be at the forefront of issues, concepts, and communities that leverage the information component of national power. We invite you to join us as we advance national security in the 21st Century.

Robert D. Childs
Director, IRM College

A Global Community of Information Leaders



"I have been dean for nearly twenty-five years at three great universities. By the reports of my faculty and by my own observation, NDU students in the Information Resources Management College are, as a group, the best prepared and most accomplished graduate students I have had the pleasure of knowing. Syracuse University faculty consider it a perk to be assigned to teach these students in our Washington, D.C. based master's program."

*Raymond F. von Dran, Ph.D.
Dean and Professor
School of Information Studies,
Syracuse University*

The IRM College offers a wide spectrum of educational activities, services, and programs to prepare information leaders who can play critical roles in national security. In every course, program, and workshop, participants 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 form a global learning community to create 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. The College offers "education in context" consistent with its mission to develop leaders who can leverage the information component for national security. These educational opportunities include workshops, presentations, and engagements to develop the government workforce to meet the needs of agencies.

Learning That Is Current, Relevant, and Future-Focused

Our faculty offer innovative curricula focusing on the relevant questions, challenges, and opportunities facing today's government leaders. While challenging students to develop their competencies in communication, critical thinking, collaboration, and leading change, 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 in their fields, who contribute unique perspectives and experiences to the learning environment.

Courses for Professional Development or Graduate Credit

IRM College offers all courses for either professional development or graduate/certificate credit. The College welcomes students who enroll in individual courses to learn and to connect with others without seeking a certificate or academic credit by electing to take a course for professional development. In such cases, a grade of Professional Development (PD) will be recorded in the student academic record and posted on the official NDU transcript. (See page 33 for more information.) Students who elect to take coursework for graduate/certificate credit will receive three semester hours of credit. NDU is accredited by the Middle States Association of Colleges and Schools.

Access to Learning Wherever You Are

To respond to the learning needs of members of its community, the IRM College offers students opportunities for face-to-face interaction, e-learning tools, online library resources, and course management software. Classrooms on campus at Fort Lesley J. McNair in Washington, D.C., (and at some off-site locations) are equipped with wireless access and laptop computers. Blackboard (Bb) supports the virtual classroom environment for all students and faculty. Online library resources are available via secure Web access from office and home. The College regularly pilots new technologies to enhance the teaching and learning process. The College provides students and their organizations with flexible learning options to accommodate their location, work schedule, and learning preferences:

- Intensive Courses, offered either in residence at Fort McNair or by distributed learning for students across the globe. (See page 36 for a description of instructional formats.)
- The Advanced Management Program (AMP), a 14-week resident program conducted at Fort McNair in Washington, D.C.
- Elective Courses, offered for AMP, National War College, the Industrial College of the Armed Forces, and School for National Security Executive Education students in residence at Fort McNair.
- Seminars, Symposia, and Workshops, and other educational activities that faculty conduct to meet particular learning needs of organizations. Occasional symposia on current seminal topics are held at Fort McNair.





“The faculty [in the course] were very professional, very knowledgeable about the subject. Excellent teachers encouraged the students to think and engage in the subject.”

“The instructor provided an environment in which learning took place from the inside: self thought and self assessment...I will retain this and apply this knowledge in the future and forever. Thanks.”

“Every course I’ve taken along the CIO Certification route has been meaningful and has provided me with a level of understanding and insights that my peers do not have. It has given me a definite advantage in my current capacity.”

The 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 conduct the College’s educational programs:

- **The Information Strategies Department** focuses on the policy and planning processes, leadership and management competencies, and perspectives for information resources management that form the foundation of the College’s CIO Certificate Program. Consistent with the Clinger-Cohen Act of 1996, the department delivers 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. The Department also conducts the Organizational Transformation Certificate Program designed to prepare individuals to leverage information and information technology to transform government.
- **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 a series of courses that emphasize security issues and approaches fundamental to the protection of the nation’s information infrastructure. The College offers three programs in Information Assurance: National Training Standard for Information Systems Security Professionals (NSTISSI No. 4011), National Information Assurance Training Standard for Senior Managers (CNSSI No. 4012), and the Chief Information Security Officer (CISO) Certificate.
- **The Systems Management Department** delivers courses and programs focused on successful application of project and program leadership skills, policies, best practices, and tools to acquire and manage the 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 Management Department conducts the Enterprise Architecture and IT Project Management Certificate programs.

The Center for Information Assurance Education

The Center for Information Assurance Education conducts 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 practice of information assurance, and conducts and disseminates research on information security, information operations, homeland security, and critical infrastructure protection.

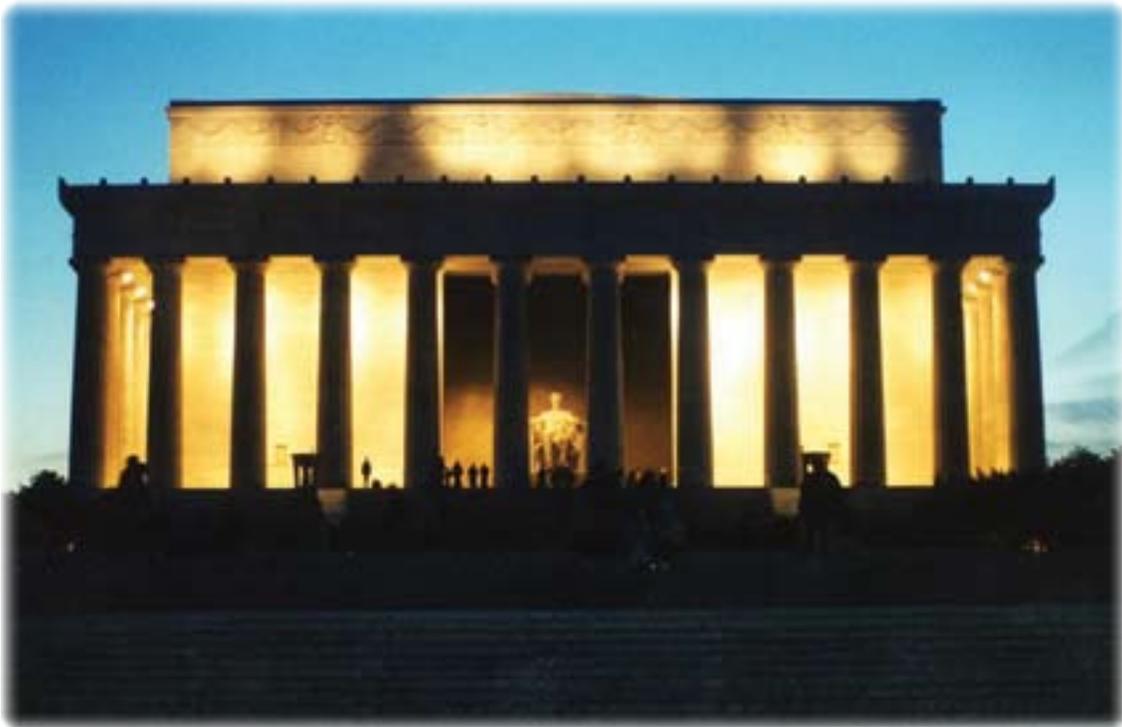
Joint Professional Military Education (JPME)

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 two 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. The student's academic advisor must approve electives taken in excess of four. Select electives may also be credited toward completion of the certificate programs offered by the College.





PROGRAMS





ADVANCED MANAGEMENT PROGRAM (AMP)

The 14-week Advanced Management Program (AMP) provides middle- and senior-level leaders with an integrated graduate-level education focused on the policies and imperatives that enable federal national security and civilian agencies to leverage information for strategic advantage. The AMP produces successful graduates who are prepared to:

- Exercise leadership in Chief Information Officer (CIO) and functional responsibilities to promote and attain national security, agency, and interagency goals;
- Balance continuity and change in development, implementation, and evaluation of information resources management strategies and policies;
- Link critical decisions regarding people, processes, and technologies to performance and results; and
- Leverage enabling technologies while assuring the security of the infrastructure.

The AMP has three elements that define its unique educational experience. First, the AMP has both core and elective courses that provide a foundation of skills and knowledge in a broad range of information resources management disciplines. All AMP students earn a CIO Certificate. AMP students focusing on Information Assurance must complete at least three of the four courses required for an Information Assurance (IA) Certificate. Information Assurance Scholarship Program students are required to complete all four courses of the IA Certificate.

Second, the program's strategic leader development curriculum provides an integrated set of learning activities that build leadership capacity and the ability to develop other strategic leaders. This curriculum focuses on enhancing leadership competencies in the areas of communication, critical thinking, leading change, and collaboration. Key components of the curriculum include individual awareness and team problem solving activities, conversations with exemplary organizational leaders, and study of and visits to a diverse set of public and private sector organizations, including an intensive week-long field study outside of Washington, D.C.

Finally, the AMP attracts senior officials from an ever-expanding variety of sponsor organizations, including the U.S. Department of Defense, foreign defense ministries, U.S. federal agencies, and private sector organizations. AMP students form a learning community that exposes them to multiple perspectives on a wide range of issues; this motivates them to share knowledge and best practices, strive to become better leaders and decision makers, and master the tools of lifelong learning. In addition, interaction with fellow students, faculty, guest speakers, and other executives provides AMP participants with a network of peers throughout the public and private sectors.

The AMP core courses are:

- **Foundations of Information Resource Management (IRM):** Presents an overview of IRM, including its concepts, policies, and their application. Lessons focus on understanding the IRM environment and the dynamic relationships among political, economic, social, fiscal, and technological forces that are changing government.
- **Information Management Planning:** Presents an approach to planning that integrates agency strategic planning, performance planning, information planning, and capital planning and investment. This course examines a comprehensive mission-driven planning framework that combines explicit and implicit planning requirements of current legislation and regulations.
- **Measures of Performance:** Provides strategies and techniques for assessing an organization's performance results as

part of strategic planning or budgeting processes. Leverages lessons learned from interagency 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.

- **Process Improvement and Investment Planning:** 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.
- **Information Technology Acquisition:** Examines the management issues that arise from policies, best practices, alignment of an acquisition with organizational goals and objectives, programmatic strategies and planning, and selection of performance metrics. This course explores several approaches for determining a suite of performance measures that will provide insights into acquisition of information technology.
- **Assuring the Information Infrastructure:** 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.



In addition to their core courses, AMP students select two elective courses. These courses enable students to broaden their knowledge or to delve deeper into the areas that are covered in the core program. For example, students can pursue studies in the areas of multimedia technologies, knowledge management, capital planning, network security, and information operations. The curriculum map illustrates the various elements of the AMP.

AMP OFFERINGS

Academic Year 2007

AMP 33: September 11 – December 14, 2006

AMP 34: January 4 – April 13, 2007; applications due October 13, 2006.

Academic Year 2008 (tentative dates)

AMP 35: September 10 – December 13, 2007; applications due June 2, 2007.

AMP 36: January 7 – April 11, 2008; applications due October 1, 2007.

AMP 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). If required, the application may also include a waiver request (see below). Omission of required information in any letter, form, or request for waiver 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 organizations worked for, position titles, 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, program the student is applying for, and if a waiver is being requested. For example: "Subj: AMP Letter of Nomination, Grade Level Waiver Request for MAJ John Doe." The final signature on all correspondence must belong to the applicant's immediate supervisor. The letter of nomination should also include a request for the student to be admitted to the CIO Certificate Program because all students who complete the AMP also satisfy the requirements for the CIO Program.
- **Waiver Requests:** Waiver requests may be included in the nomination letter. The subject line and first paragraph of the letter should clearly state that the applicant's supervisor is requesting a waiver of the eligibility criteria. The request must fully describe the applicant's job background, current position, the organization's need for the applicant's participation in the program, and any equivalent experiences or academic credentials that support consideration of the waiver.

Applications can be submitted 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 Lesley J. McNair
Washington, D.C. 20319-5066.

State and Local Government: State and local government applications for AMP must include a résumé, a letter of nomination from a direct supervisor, and a completed copy of the AMP application form.

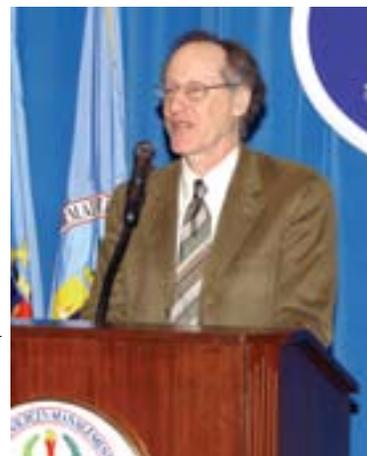
Private Industry: Private industry applications for AMP must include a résumé, a letter of nomination from a direct supervisor, and a completed copy of the AMP application form.

International Students: Non-U.S. citizens who are members of international defense agencies must apply through their governments. Applications should be in the form of an education and training request for approval and processing through the appropriate 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: ATFA-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 English language competency via the Defense Language Institute's English Level Comprehension (ELC) Exam administered in the home country prior to acceptance. The IRM College reserves the right to administer the exam when 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.

The Advanced Management Program Director, Dr. Kathleen Schulin, can be contacted at schulink@ndu.edu.



Steven Kelman, Weatherhead Professor of Public Management, Harvard University's John F. Kennedy School of Government

The Chief Information Officer (CIO) Certificate Program, sponsored by the DoD CIO, is the recognized source of graduate education for Federal CIO leaders to develop themselves and their agency personnel for leveraging 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). CIO Program graduates earn an official certificate, signed by the DoD CIO and the Director of IRM College that recognizes they have earned an education in the Federal CIO competencies. Graduates earn an equivalent of 15 graduate credit hours toward selected master’s or doctoral degree programs at partnering institutions of higher education.



Figure 1

The CIO Certificate Program is organized around 11 subject areas directly related to CIO competencies identified by the Federal CIO Council (see Figure 1). Each of these subject areas contains multiple courses that students can select to tailor their CIO program of study to meet their organization’s needs and priorities (see Figure 2).

CERTIFICATE REQUIREMENTS

Courses in each competency are designated as “Core” because of their breadth and necessary links to the CIO competency or “Specialty” because of their depth in a particular competency. Students work with their supervisors and academic advisors 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 courses which satisfy the following:



John G. Grimes
Assistant Secretary of Defense for Networks and Information
Integration/DoD Chief Information Officer

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

All courses, independent of the format in which they are offered, provide students academic content and intellectual rigor. Students have four years from the date of their acceptance into the CIO Certificate Program to complete the requirements and must successfully complete at least one course every 18 months to maintain active status in the program.

Figure 2: CIO Certificate Program Requirements

Required Core Courses (3 Courses)		
Key Competency Area	Course (Catalog Number)	Course Title
Policy	CWC (6317)	<i>Changing World of the CIO</i>
Performance- and Results-Based Management	MOP (6316)	<i>Measuring Results of Organizational Performance</i>
Security and Information Assurance	All (6203)	<i>Information Assurance & Critical Infrastructure Protection</i>

Additional Core Courses (3 Courses from 3 different Key Competency Areas)		
Key Competency Area	Course (Catalog Number)	Course Title
Acquisition	ITA (6415)	<i>Strategic Information Technology Acquisition</i>
Architecture and Infrastructure	ARC (6409) DMS (6414)	<i>Enterprise Architectures for Managers Data Management Strategies and Technologies: A Managerial Perspective</i>
Capital Planning and Investment	BBC (6430) MTI (6315)	<i>Building an IT Business Case IT Capital Planning</i>
eGovernment / eBusiness	EGV (6525)	<i>eGovernment</i>
Leadership	LDC (6301)	<i>Leadership for the Information Age</i>
Process Improvement	PRI (6333)	<i>Strategies for Process Improvement</i>
Strategic Planning	IMP (6318) IWS (6202)	<i>Information Management Planning Information Warfare and Military Strategy (Secret Clearance Required)</i>
Technology Assessment	CST (6510)	<i>Critical Information System Technologies</i>

Other Courses (2 Courses)		
Any course from the College Catalog		



ENTERPRISE ARCHITECTURE (EA) CERTIFICATE

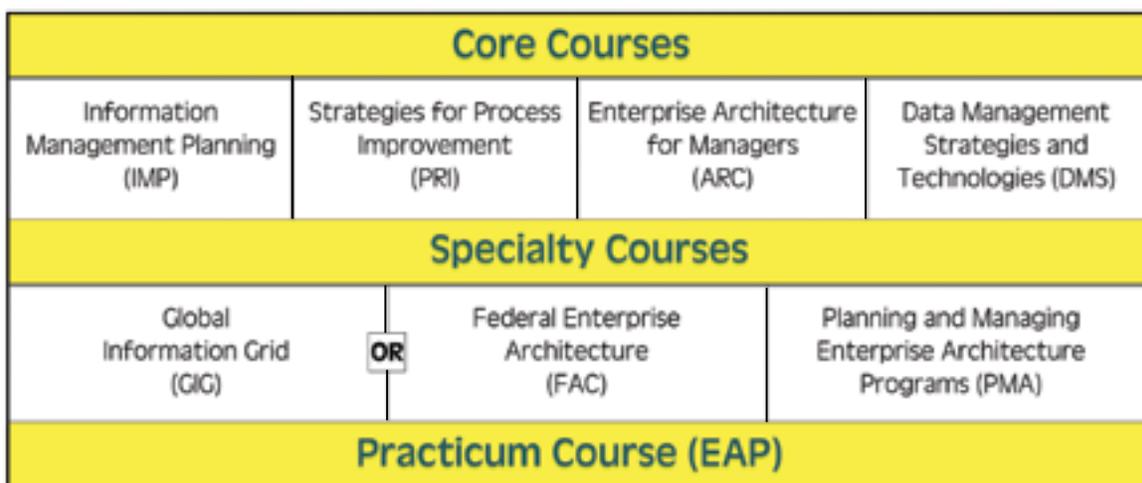
The Enterprise Architecture (EA) Certificate builds competencies to enable agencies to meet their Clinger-Cohen Act responsibilities for “developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture.” The program provides graduate-level education organized around seven core EA competencies determined by the Federal CIO Council (see figure below). EA Certificate students develop skills in both policy and technical aspects of developing, implementing, and maintaining an EA. They also are enabled to apply EA concepts and processes to support strategic planning and realize organizational and process transformation.

Certificate students learn EA development approaches to achieve mission improvement and business value rapidly, aid development of business cases, and implement strategies to achieve sustained interoperability.

Enterprise Architecture Certificate graduates understand and can apply and implement 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 Net-Centric Operations Warfare Reference Model (NCOW RM)
- OMB and the CIO Council’s Federal Enterprise Architecture (FEA) Reference Models, the Federal Enterprise Architecture Framework (FEAF)
- Industry-based EA frameworks (e.g., Zachman)

Award of the Enterprise Architecture Certificate requires successful completion of four core and three specialty courses. The four core courses are *Enterprise Architecture for Managers* (ARC), *Information Management Planning* (IMP), *Strategies for Process Improvement* (PRI), and *Data Management Strategies and Technologies* (DMS). Specialty courses required for award of the certificate are *Planning and Managing Enterprise Architecture Programs* (PMA) and either the DoD-oriented *Global Information Grid Architecture* (GIG) course or the civilian agency-oriented *Federal Enterprise Architecture* (FAC) course. ARC must be successfully completed before enrolling in PMA, GIG, or FAC. As the final course in the Enterprise Architecture certificate, students complete the *Enterprise Architecture Practicum* (EAP), integrating knowledge and skills acquired in their prior courses through application in an organizational setting.





The Information Assurance (IA) Certificate Programs consist of a series of courses 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 being compliant with national the IA education and training standard (NSTISSI No. 4011) for Information Systems Security Professionals. The CNSS has also certified the curriculum as being compliant with the national IA education and training standard (CNSSI No. 4012) for Senior System Managers, who include the Chief Information Officer (CIO), Designated Approving Authority (DAA), and Chief Technology Officer (CTO), etc. These certificates also satisfy the DoD 8570.1-M (paragraph C1.4.4.13) education requirements for management personnel performing IA functions on national security systems.

The Chief Information Security Officer (CISO) Certificate is a source of graduate-level information security education for senior agency information security officers, 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 doctorate degree programs at several partner institutions of higher education.

CERTIFICATE REQUIREMENTS

NSTISSI No. 4011 Certificate Requirements: Participants in the 4011 Certificate have up to four years from the date of acceptance to complete the program. This certificate requires completion of the following four courses:

- *Information Assurance and Critical Infrastructure Protection (AII)*
- *Global Enterprise Networking and Telecommunications (GEN)*
- *Managing Information Security in a Networked Environment (SEC)*
- *Enterprise Information Security and Risk Management (ESS)*



Hun Kim, Deputy Director National Cybersecurity Division, DHS

*John Saunders, Director Center for IA Education
Mary Polydys, Chair, Information Operations and Assurance Department*

It is strongly recommended that the AII and GEN courses be taken first, followed by SEC and ESS. Successful completion of three of these four courses may be applied toward requirements for the CIO Certificate Program. Students in the Advanced Management Program also have the opportunity to qualify for the 4011 certificates.

CNSSI No. 4012 Certificate Requirements: This certificate requires completion of five courses, the four listed above for the 4011 Certificate plus a fifth course, *Approval to Operate (ATO)*. Participants in the 4012 Certificate have four years to complete the program.

Chief Information Security Officer (CISO) Certificate Requirements: This certificate requires completion of eight courses, the five courses for the 4011 and 4012 certificates plus three additional courses. Participants in the CISO Certificate have up to four years from the date of acceptance to complete the program.

- *Information Assurance and Critical Infrastructure Protection (AII)*
- *Global Enterprise Networking and Telecommunications (GEN)*
- *Managing Information Security in a Networked Environment (SEC)*
- *Enterprise Information Security and Risk Management (ESS)*
- *Approval to Operate: Information System Certification and Accreditation (ATO)*
- *Cyberlaw (CBL)*
- *Continuity of Operations (COO)*
- *One of the following:*
 - *Homeland Security Information Management (HLS)*
 - *Homeland Security Tools and Technologies (HST)*
 - *Managing Security of Control Systems (SCS)*
 - *Information Operations and National Security in the Information Age (IOS)*
 - *Privacy Rights and Challenges in the Information Age (SPA)*
 - *Strategic Management of Software Assurance (SAA)*
 - *Protection of Critical Infrastructure and Key Assets (CIP)*





The Information Resources Management College now offers an Information Technology Project Management (IT-PM) Certificate program to assist agencies in complying with Office of Management and Budget direction that project managers qualified in accordance with CIO Council guidance manage all major information technology projects. The IT-PM 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) Certificate¹.

The IT-PM 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 first-rate 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.

CERTIFICATE REQUIREMENTS

Award of the Information Technology Project Management Certificate requires completion of three core courses and three specialty courses. The core courses are *Strategic Information Technology Acquisition (ITA)*, *Critical Information Systems Technologies (CST)*, and *Building an IT Business Case (BBC)*.

Three specialty courses are required: *Information Technology Project Management (ITP)*, *Software Acquisition Leadership (SAL)*, and *Information Technology Project Leadership (IPL)*.

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

¹ 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 <http://www.pmi.org>.



ORGANIZATIONAL TRANSFORMATION (OT) CERTIFICATE

The environment is no longer predictable, characterized by small shifts, or changing at a measured pace. The explosive growth of technology innovations, economic globalization, and democratization of information have created a world of high complexity, interdependence, and uncertainty. Disruptive and unpredictable changes will affect all aspects of organizations, often all at once. Successful and significant organizations will embrace the opportunity to transform, either by responding to or shaping the new environment to accomplish mission goals, stretch their visions, and sustain strategic advantage.

The new Organizational Transformation (OT) Certificate is designed to develop leaders who can shape the environment and their organizations through transformation. Government organizations at all levels - federal, state, and local - are challenged to transform. The Organizational Transformation Certificate offers government decision-makers and staff the opportunity to develop their acuity about the nature, forces, and dependencies and interdependencies of turbulent and unpredictable environments, and about the levers and tools for organizational transformation. The course of study, focused on people, processes, and technology, allows them the opportunity to expand their creative and critical thinking on strategies, governance, organizational designs, processes, networks, and tools in ways that will enable them to leverage information and information technologies to achieve their mission while creating and sustaining strategic competitive advantage.



The Organizational Transformation Certificate is organized around three required courses that target the heart of organizational transformation: the dynamic environment and governance (*Transformation as Strategic Alignment*), networking and multi-agency collaboration (*Multi-Agency Information-Enabled Collaboration*), and creativity and disruptive innovation (*Leading Strategies for Disruptive Innovations*). The specialty courses allow students to explore particular aspects of Defense and National Security, Homeland Security, and National Preparedness.

OT Certificate Replaces eGovernment Leadership Certificate

The Organizational Transformation Certificate Program replaces the eGovernment Leadership Certificate Program. Students currently enrolled in the eGovernment Program may choose to complete that certificate or transfer to the new program. They will receive full credit for all courses taken in the eGovernment Program.

CERTIFICATE REQUIREMENTS

Award of the Organizational Transformation Certificate requires successful completion of eight courses. Three required courses: *Transformation as Strategic Alignment (TAS)*, *Multi-Agency Information-Enabled Collaboration (MAC)*, and *Leading Strategies for Disruptive Innovations (LSI)*. Students can select five additional courses from the Organizational Transformation specialty courses.

In subsequent academic years, the college may add or delete choices in the areas of specialization; however, students will receive credit for courses already taken in the program. Participants have up to four years from the date of acceptance to complete the program and must successfully complete at least one course every 18 months to remain active.

Students admitted to the Organizational Transformation Certificate during AY 2005-2006 will follow the requirements in the *AY 2005-2006 IRM College Catalog* or may elect to follow the program as outlined in this catalog.



Zal Azmi
Chief Information Officer
Federal Bureau of Investigation

Eligible individuals who wish to take intensive courses without participating in an IRM College certificate program may apply at any time by submitting a completed application and required documents.

NO MORE THAN two courses taken for credit through General Studies may be applied toward a certificate. Students interested in only taking courses as professional development may apply to the College as General Studies instead of a particular certificate program.





ADMISSIONS POLICY

The IRM College is solely responsible for determining its admission criteria and for determining which applicants are admitted. Questions concerning admission should be addressed to the Registrar's Office either by phone (202-685-6300; DSN 325-6300) or by e-mail (IRMRegistrar@ndu.edu).

The IRM College uses the National Defense College's uNET, an online student admission and enrollment management system. uNET has replaced most traditional paper-based and in-person transaction processes. (Link to uNET through the IRM College homepage at <http://www.ndu.edu/irmc>.)

- o To enroll, students must be admitted to the IRM College and be accepted into one or more academic programs.
- o Students have four years from the date of their acceptance into a certificate program to complete the requirements. (Exception: Information Assurance Scholarship students must complete the IRM College portion of their studies in two years.)
- o All coursework applied toward a certificate must be completed within the previous four years. Students must successfully complete at least one course every 18 months to maintain active status in the program.

IRM College academic programs are:

- The Advanced Management Program (AMP)
- The Chief Information Officer (CIO) Certificate Program
- The Enterprise Architecture (EA) Certificate Program
- The Information Assurance (IA) Certificate Program NSTISSI No. 4011
- The IA Certificate Program CNSSI No. 4012
- The Chief Information Security Officer (CISO) Certificate Program
- The Information Technology (IT) Project Management Certificate Program

- The Organizational Transformation (OT) Certificate Program
- General Studies: This is not a certificate program.

ELIGIBILITY CRITERIA

Pay Grade or Rank: Federal civilian government employees must be at least GS/GM-13 or equivalent, and military officers must hold at least the grade of O-5. Non-federal students, to include state and local government and private sector employees, must be of an equivalent grade.

Note: Private sector employees must be sponsored by a government agency.

Education: All students must possess a bachelor's degree from a regionally accredited institution.

Exceptions: Requests for waivers are considered for applicants who are within one grade level of the minimum eligible grade or who do not meet the minimum education requirement.

Change in Eligibility: The College will periodically review eligibility. If a student's eligibility criteria changes (employer, pay grade, rank, etc.), he/she must notify the College. In cases where eligibility ceases, course credit earned while in an ineligible status may be revoked and/or the student may be held liable for tuition owed.

Requests to Waive Eligibility Requirements

Waiver requests may be included in the Employer Verification Letter, Private Sector Sponsorship Letter, or may be on organizational or corporate letterhead and be addressed to the Dean of Students and Administration. The final signature must belong to the most immediate supervisor or Human Resources Officer holding a grade of GS/GM-13, O-5, or higher.

The request must fully describe the applicant's job background, current position, the organization's need

for the applicant's participation in the program, and any equivalent experiences or academic credentials that support consideration of the waiver.

Submission of supporting documents for admissions applications may be made to the IRM College Registrar via fax (202-685-4860) or electronically as a scanned e-mail attachment sent to IRMCRegistrar@ndu.edu.

Failure to submit required information in any letter or request for waiver consideration may result in denial of the request. Incomplete applications will be held by the IRM College for 60 days.

APPLICATION INSTRUCTIONS - Overview

All students must apply to the IRM College to enroll in classes. Students may apply for and be admitted to more than one IRM College academic program at a time. All coursework applied toward a certificate must be completed within the previous four years. No more than two courses taken while in the General Studies may be applied toward a certificate.

Application Processing Overview

When the Registrar's Office receives an application, the applicant is sent a confirmation e-mail. The application is then reviewed for eligibility and required documents. If a document is required (and not already in the office), an e-mail is sent to the applicant. Once all documents are received, the application is reviewed and an admission decision is reached. Once successfully admitted, the applicant is sent notification. (New students will also be sent a uNET Username and Password by e-mail, which he/she will use to register for courses in uNET.) If not admitted, the applicant will be sent notification.

Application Overview		
	Programs (non-AMP)	AMP
ADMISSION		
Application	Electronic, via uNET	Paper
Résumé required	No	Yes
Employer Verification Letter required	Yes, excluding Private Sector (industry) Applicants	No
Private Sector Sponsorship Letter-required	Private Sector (industry) applicants only	No
Nomination Letter required	No	Yes
Non U.S. Citizen Admission	No	Yes
VERIFICATIONS		
<i>Required upon Request</i>	Identity, education, employer, grade/rank	

Processing Time

uNET will send a confirmation message to applicants who successfully submit an online application. All applications are reviewed for completeness and applicant eligibility within 5-7 business days of receipt. The average admission processing time for a complete application is 10-15 business days. Applicants will receive feedback by e-mail if further documentation is required to complete the application package. Incomplete applications will be held by the IRM College for 60 days and then destroyed. Students who need assistance with accessing uNET or completing an IRM College application should contact the Registrar's Office by phone (202-685-6300, DSN 325-6300), or by e-mail IRMCRegistrar@ndu.edu.

Employer Verification Letter Template

GENERAL APPLICATION

INSTRUCTIONS (Excluding AMP; see AMP section for detailed instructions.)

STEP ONE: Submit your application online.

The IRMC Application for Admission is available from the uNET Guest Page or, for prior/current students, through an existing uNET account (link to uNET through the IRM College homepage at <http://www.ndu.edu/irmc>).

Note to current/returning students applying via uNET: Applying through uNET requires a uNET Username and Password. If you forgot/need the Username and Password, you must submit a request to the uNET help desk at ITSG@ndu.edu.

Note: Returning students who are seeking RE-ADMISSION to an IRM College program should include a request for reinstatement along with justification or explanation of extenuating circumstances to IRMCEXceptionRequest@ndu.edu. Reinstatement to a certificate program may be granted on a case-by-case basis. A response will be sent by e-mail to the address originating the request.

STEP TWO: Submit required documents

(employer verification, endorsement and/or waiver letters).

Letters and other application documents may be submitted to the IRM College Registrar via fax (202-685-4860) or electronically as a scanned e-mail attachment sent to IRMRegistar@ndu.edu. Incomplete applications will be held by the IRM College for 60 days, and then destroyed.

a. All Applicants (excluding Private Sector): Employer Verification Letter

The applicant's most immediate supervisor or Human Resources Officer holding a grade of GS/GM-13, O-5, or higher must complete and submit the following list, printed on organizational letterhead, directly to the IRM College (fax: 202-685-4860 or scanned attachment to IRMRegistar@ndu.edu). The employer representative may attach additional comments. A downloadable version of the letter template is available on the IRM College website (www.ndu.edu/irmc).

• Applicant Information:

1. Applicant Name:
2. Organization Name:
3. Job Title:
4. Grade/Rank:

• Employer Representative (Supervisor or HR Officer) Information:

5. Name:
6. Organization Name:
7. Job Title:
8. Grade/Rank:
9. Address:
10. City, State, Postal Code:
11. Telephone/Ext:
12. DSN:

• Eligibility:

13. Grade/Rank: The applicant's position is equivalent to **GS/GM 13 or O-5** or above:
___ Yes ___ No/uncertain
14. Education: The applicant has earned at least a bachelor's degree from a regionally accredited institution:
___ Yes ___ No/uncertain
15. If you answered No/uncertain to either #1 or #2, please complete (a) and (b) below to recommend a waiver of eligibility criteria:
(a) Describe the current 'level of responsibility' (senior level management, supervisory, etc.):
(b) Provide a brief description of the core responsibilities of the applicant's position (or attach a description):

• Certification:

16. Employer Representative Signature:
17. Date (mm/dd/yy):

b. Private Sector Applicants ONLY: Private Sector Sponsorship Letter

Private sector employee applications must include an endorsement letter from the sponsoring government agency's contract coordinator (or his/her most immediate supervisor) holding a grade of GS/GM-13, O-5, or higher (or equivalent grade level for state/local government). The sponsor must complete and submit the following

list, printed on organizational letterhead, directly to the IRM College (fax: 202-685-4860 or scanned attachment to IRMCRegistrar@ndu.edu). A downloadable version of the letter template is available on the IRM College website (www.ndu.edu/irmc).

<i>Private Sector Sponsorship Letter Template</i>	
<ul style="list-style-type: none"> • Applicant Information: <ol style="list-style-type: none"> 1. Applicant Name: 2. Organization Name: 3. Job Title: • Sponsor Information: <ol style="list-style-type: none"> 4. Sponsor Name: 5. Organization Name: 6. Job Title: 7. Grade/Rank: 8. Address: 9. City, State, Postal Code: 10. Telephone/Ext: 11. DSN: • Assessment: <ol style="list-style-type: none"> 12. The number of the contract being supported: 13. The applicant is a U.S. citizen: ___ Yes ___ No 14. The applicant is performing work directly supporting the scope of a valid government agency contract: ___ Yes ___ No 15. There is a valid government agency requirement for the requested education: ___ Yes ___ No 16. Grade Level: Equivalent to GS/GM 13: ___ Yes ___ No/uncertain 17. Education: The applicant has earned at least a bachelor's degree from a regionally accredited institution: ___ Yes ___ No/uncertain 18. If you answer No/uncertain to either #16 or #17, please complete (a) and (b) below to recommend a waiver of eligibility criteria: <ol style="list-style-type: none"> (a) Describe the current 'level of responsibility' (senior level management, supervisory, etc): (b) Provide a brief description of the core responsibilities of the applicant's position (or attach a description): • Certification: <ol style="list-style-type: none"> 19. Signature: 20. Date (mm/dd/yy): 	

c. Waiver Letter:

See REQUESTS TO WAIVE ELIGIBILITY REQUIREMENTS section above. Submit only if applicable.

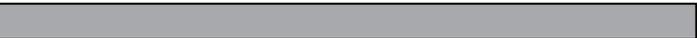
STEP THREE: Receive program acceptance notification.

IRM College Admissions Committee: The IRM College Admissions Committee meets weekly to review complete applications. Questions concerning status of pending applications should be addressed to the Registrar's Office at 202-685-6300, DSN 325-6300, or IRMCRegistrar@ndu.edu.

Communications of IRM College Admission Committee Decisions: Applicants to programs will receive both an e-mail notification and a formal letter to notify them of the IRM College Admissions Committee decision regarding their application. Communications will detail the applicant's program status, the official start and end dates of their program and contact information for their faculty advisor. Advanced Management Program selectees are notified of acceptance normally at least seven weeks before the beginning of the session.

STEP FOUR: Receive notification of your faculty advisor.

Students admitted to any IRM College academic program leading to a certificate are assigned a faculty advisor. Advisors are available to help the student plan a course of study and answer questions about program requirements.



FEES

There are no fees for DoD employees for IRM College courses or programs. This includes all course offerings and the Advanced Management Program, but may not include special offerings such as executive or special seminars. DoD students interested in special offerings should check the IRM College website for applicable fees.

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.

FY07: The FY 2007 intensive course fee for non-DoD federal, state, and local government employees is \$1,100. The FY 2007 intensive course fee for private industry students is \$1,995.

FY07: The Advanced Management Program (AMP) fee for non-DoD federal, state, and local government employees is \$10,500. The fee for private industry students is \$16,500.

PAYMENT INSTRUCTIONS

All payments for intensive classes are due no later than the first day of class. If payment is not received, the student's account will be delinquent, the student may not be admitted to the class and the student will not be allowed to attend future classes until his/her account is cleared.

All payments for students enrolled in AMP are due prior to the first day of the AMP. If an AMP student's payment is not received, the student will be asked to reapply for a future offering.

IRM College cannot accept cash payments. Valid forms of payment are: credit card, check, electronic funds transfer, or Military Interdepartmental Purchase Request (MIPR). Students are advised to fax or bring proof of payment in the form of a "print screen" showing the transaction has been processed by their organization.

Detailed instructions for submitting payment will be provided to the student by e-mail and in the student's invoice when the student is accepted into a class.

COURSE REGISTRATION

Enrollment Procedures

Once accepted into an academic program, the student will be assigned a student account, Username and Password which he/she will use to self-enroll in classes from the NDU student information system, uNET (link from www.ndu.

edu/irmc). If a student experiences any problems accessing accounts or enrolling in classes, he/she may contact the Registrar's Office at 202-685-6300 or IRMCRegistrar@ndu.edu.

Enrolling With the Class Number

The Class Number can be found next to each class offering listed in the class schedule. It is a four-digit number and it is the unique identifier for each class in that Academic Year.

1. Log into uNET (using your Username and Password)
2. Under the Enterprise Menu (left side), click on "Learner Services Home"
3. Click on "Add/Drop a Class"
4. Select "Academic Year 200X/200X"
5. Select "Add Classes"
6. Enter Class Number
7. Click "Submit"
8. Click "View My Schedule"

Enrolling Without the Class Number

If you do not have the Class Number, or if you would like to search the system for open classes, do the following:

1. Log into uNET (using your Username and Password)
2. Under the Enterprise Menu (left side), click on "Learner Services Home"
3. Click on "Add/Drop a Class"
4. Select "Academic Year 200X/200X"
5. Click on the magnifying glass next to the Class Number box
6. In the Subject box, enter "IRMC-INT"
7. In the Description box, enter the three letter course description (e.g., ARC, GEN, SEC, etc.)
8. Optional: Notice that the "Open Classes Only" box is checked. That means that the search will return only open classes. If you want to see all classes (e.g., you may want to place yourself on the wait list), click inside the box to remove the check.
9. Click on "Search"
10. Click on the checkbox next to the class you want to attend
11. Click "Submit"
12. Click "View My Schedule"

To complete the enrollment process, non-DoD students must fax a training form (SF 182 or equivalent) to the Registrar's Office at 202-685-4860.

8. Click "Submit"
9. Click "View My Schedule"

Confirmation of Enrollment

Students may confirm successful enrollment by viewing their course schedule from their Learner Services Home page. Students who successfully enroll in a course will be sent a course acceptance notice automatically from uNET. Additional reminders and attendance confirmation requests may be sent prior to the course start date.

Precourse Materials and Assignments

Each course has Blackboard-accessible readings and other precourse activities that allow students to prepare for the first day of their course. Precourse 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

Students who do not disenroll (via uNET, the Registrar's Office, or the Offering Leader) by the start date will be assigned an enrollment action of "No Show" (NS). After the second "NS", students will be prohibited from taking courses for six months.

Dropping a Course in uNET:

If your schedule prevents your participation in a scheduled course, we request you cancel yourself in uNET. [Special agreement (MOA) students: Students attending courses under a special agreement (MOA) should follow their agency's local procedures to coordinate changes or cancellations.]

1. Log into uNET (using your Username and Password)
2. Under the Enterprise Menu (left side), click on "Learner Services Home"
3. Click on "Add/Drop a Class"
4. Select "Academic Year 200X/200X"
5. Select "Drop/Update Classes"
6. You will now see all classes you are enrolled in
7. Select "Drop" in the Action field next to the class or classes that you are dropping



OTHER STUDENT SERVICES

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 are correct in uNET to assist the IRM College in meeting federal and Department of Defense directives and reporting requirements.

Certification of Program Completion

The Registrar's Office will issue a program completion letter signed by the Director. Successful completion of an IRM College certificate program may be verified with a program completion letter or an original National Defense University official transcript. The date noted in the program completion letter or program completion date shown on the 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.

Certificate Issuance

Program certificates are prepared yearly for the IRM College's graduation exercise. The IRM College will mail certificates to students who cannot attend the graduation ceremony. Students are responsible for maintaining mailing and shipping addresses in uNET to ensure delivery is not delayed.

Reprinting Certificates

IRM College certificates note satisfactory completion of a graduate-level program. Only one certificate will be produced per program per student. Students should safeguard their certificate(s) as they would other important documents.

In exceptional cases, the IRM College will reproduce certificates for a student; however, the College cannot guarantee signatures from the original signers. Students with an exceptional case (i.e., lost in a fire) may contact the Registrar's Office via e-mail at IRMCRegistrar@ndu.edu for further guidance.

Graduation Exercises

The IRM College Graduation Exercise for Academic Year 2007 is tentatively scheduled for April 13, 2007 (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 six 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 of graduation are advised to work closely with their faculty advisor and course instructors to ensure they meet requirements in time for graduation. All students must meet their program(s) requirements no later than March 30, 2007 for the April ceremony.

Transcripts

Two types of transcripts are available from the IRM College.

Unofficial Transcripts. Students with an account on uNET can print unofficial transcripts from their "Learner Services" home.

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 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/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.

ACADEMIC ADVISING AND POLICIES

Faculty Advisors

Students admitted to any IRM College academic program leading to a certificate are assigned a faculty advisor. Advisors are available to help students plan a course of study and answer questions about program requirements.

Admission to Multiple Academic Programs

Students may apply for and be admitted to more than one IRM College academic program at a time. All coursework applied toward a certificate must be completed within the previous four years.

Applying Coursework Earned Prior to Program Admission

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

four years. No more than two courses taken while in the General Studies earned for credit may be applied toward a certificate.

Requests for exception to the application of previous IRM College academic work to a new program may be e-mailed with a justification to IRMCExceptionRequest@ndu.edu. Response will be made by e-mail to the address originating the request.

Completing the Certificate Program

Students are encouraged to maintain contact with their faculty advisor throughout their program of study, but particularly as they near completion of their certificate program(s). When students complete the last course needed for the program certificate, they should notify their advisor by e-mail that the requirements are satisfied. Advisors will then review records to ensure that all program requirements are met and certify completion of the program(s).

Other Certificate Program Actions

Drop. Students may be dropped from an IRM College certificate program for a number of reasons that include, but are not limited to, failure to successfully complete a class within an 18-month period; program not completed within four years from date of acceptance; earning multiple grades of “No Credit;” or decision of the Academic Review Board.

Withdrawal. Students who wish to end their participation in an IRM College certificate program may submit a signed request to the Registrar. The request should state the student’s name, e-mail address (if different than posted in uNET), program(s) from which the student wishes to withdraw, a brief justification statement, and the student’s signature. Requests may be faxed to the Registrar, Attn: Program Clerk at 202-685-4860 or e-mailed as a scanned attachment to IRMCRegistrar@ndu.edu. Confirmation of withdrawal will be provided by e-mail.

Reinstatement. Reinstatement to a certificate program may be granted on a case-by-case basis. Students who wish to request reinstatement must e-mail their request along with justification or explanation of extenuating circumstances to IRMCExceptionRequest@ndu.edu. A response will be sent by e-mail to the address originating the request.

GRADING

Beginning with the 2005/2006 Academic Year, the IRM College implemented a new grading system as 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.
 - 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/she must request it in writing to the faculty member who is 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. The student normally is given one to two weeks to resubmit the academic requirement.
- In either case, the highest possible final grade the student can obtain is a B+. A student 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 class after the start date but within the first 25 percent of the class, the faculty member will assign a grade of “W”. The request to withdraw must be submitted in writing to the Offering Leader of the class. 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 expects all requirements submitted by each student to be original work, produced by the student for the first time while a student 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. Work submitted cannot be a modification of a paper or presentation submitted for a previous course, and must contain the student’s own ideas except as correctly and fully cited. For details on the college standards for academic papers, the IRM College Publication Guidelines are available on the website.

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. The college is currently screening submitted assessment products using plagiarism detection software.

Another aspect of academic integrity involves academic and professional credentials. Students are required to provide accurate and documentable information about their educational and professional backgrounds. If a student is admitted to the College with false credentials, he or she will be sanctioned.

Suspected violations of the academic integrity policy of the IRM College are referred to the Academic Review Board. Sanctions range from expulsion, suspension, revocation of certificates, a grade of “no credit” with a transcript notation of “academic dishonesty,” rejection of the work submitted for credit, or a letter of admonishment. The final authority for decisions and actions rests with the College.

The student’s sponsoring service or organization may be notified about a violation of the College’s Academic Integrity policy which may have serious consequences for his or her security clearance and continued employment.

COURSE EVALUATION

Student feedback is a critical component of the IRM College's efforts to offer current, relevant, and high-quality courses and programs. At the end of each course offering the students are urged to submit their comments on the course and various aspects of its design and delivery. The end-of-course survey provides students the opportunity to provide feedback on the instruction, materials, and intended learning outcomes. Survey results are shared with the faculty and the college leadership and are used as a basis for future course revisions.

INSTRUCTIONAL FORMATS

Intensive courses are available in two formats:

- The **e-Resident** format uses a blended approach to engage learners in various learning activities:
 - Precourse materials in Blackboard (Bb): Students may access course materials up to 13 days prior to the start date of the course virtually 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 portion: Students enrolled for certificate/graduate credit must complete an end-of-course assessment. This assessment normally 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.)

- **The Distributed Learning (DL)** format engages students virtually in 10 to 12 weeks of instruction in Bb, use of online library resources, and assignments with faculty and other students using Bb for communication and interaction.
 - Graded assessment portion: Students enrolled for certificate/graduate credit

must complete an end-of-course assessment. This assessment normally 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 instructional period.)

- NOTE: Students may not enroll in more than two DL courses at a time.

PROFESSIONAL DEVELOPMENT

IRM College offers all courses for either professional development or graduate/certificate credit. The College welcomes students who enroll in individual courses to learn and to connect with others without seeking a certificate or academic credit by electing to take a course for professional development. In such cases, a grade of Professional Development (PD) will be recorded in the student academic record and posted on the official NDU transcript. Students in certificate programs may take courses for a PD grade; however, for a course to count toward a certificate or as a prerequisite, it must be taken for credit.

Students taking courses for professional development will:

- declare their intent to take a course for professional development, and
- complete attendance and participation requirements for the course as outlined by the offering leader.

COURSE DESCRIPTIONS



All courses may be taken for graduate/certificate credit or professional development.

DESCR.	COURSE TITLE	CATALOG NUMBER
All	Information Assurance and Critical Infrastructure Protection	6203
ARC	Enterprise Architectures for Managers	6412
ATO	Approval to Operate: Information System Certification and Accreditation	6209
BBC	Building an IT Business Case	6430
CBL	Cyberlaw	6204
CIP	Protection of Critical Infrastructure and Key Assets	6212
COO	Continuity of Operations	6504
CST	Critical Information Systems Technologies	6510
CWC	The Changing World of the CIO	6317
DBE	Defense Business Enterprise Transformation	6501
DMS	Data Management Strategies and Technologies: A Managerial Perspective	6414
DTF	Defense Transformations	6509
EAP	Enterprise Architecture Practicum	6413
EGV	eGovernment	6505
ESG	Experimentation, Simulation, and Gaming: Testbed for Transformation	6502
ESS	Enterprise Information Security and Risk Management	6206
FAC	Federal Enterprise Architecture and Advanced Concepts	6409
GEN	Global Enterprise Networking and Telecommunications	6205
GIG	Global Information Grid Architecture and Advanced Concepts	6434
HLS	Homeland Security Information Management	6507
HST	Homeland Security Information Management: Tools and Techniques	6503
ICS	Information Engagement and Strategic Communication	6208
IMP	Information Management Planning	6318
IOS	Information Operations and National Security in the Information Age	6207
IPL	Information Technology Program Leadership	6411
ITA	Strategic Information Technology Acquisition	6415
ITP	Information Technology Project Management	6416
IWS	Information, Warfare, and Military Strategy	6202
KMI	Knowledge Management and Information Sharing	6506
LDC	Leadership for the Information Age	6301
LSI	Leading Strategies for Disruptive Innovation	6511
MAC	Multi-Agency Information-Enabled Collaboration	6512
MOP	Measuring Results of Organizational Performance	6316
MTI	Information Technology Capital Planning	6315
NCW	Network Centric Warfare and Operations	6513
PMA	Planning and Managing Enterprise Architecture Programs	6432
PRI	Strategies for Process Improvement	6333
SAA	Strategic Management of Software Assurance	6211
SAL	Software Acquisition Leadership	6410
SCS	Managing Security of Control Systems	6210
SEC	Managing Information Security in a Networked Environment	6201
SPA	Privacy Rights and Challenges in the Information Age	6508
TAS	Transformation as Strategic Allignment	6528

AII

INFORMATION ASSURANCE AND CRITICAL INFRASTRUCTURE PROTECTION

Subject: IRMC-INT
Catalog Number: 6203

COURSE DESCRIPTION

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.

RECOMMENDED ATTENDANCE

This course is appropriate for senior leaders who exploit the information component of national military and economic power. This includes, but is not limited to, government and military information operators; Chief Information Officers; Chief Information Security Officers; military and government personnel who develop and manage information resources; and students in Professional Military Education programs (intermediate and senior).

PREREQUISITES

None; however, it is strongly recommended that this be the first NSTISSI No. 4011 certificate course taken.

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 ARCHITECTURES FOR MANAGERS

Subject: IRMC-INT
Catalog Number: 6412

COURSE DESCRIPTION

This course examines enterprise architecture (EA) as a management tool to facilitate implementation of strategic direction. This includes exploring the integration of EA with strategic and resource planning, information assurance, and acquisition management. It introduces the use of EA frameworks to improve the capability maturity level of the EA to meet its intended purpose. Other topics include the role of the CIO in EA management, the use of models and standards, implementation issues, and an overview of enterprise information assurance/security architecture. Strategies are also addressed for using EA to address enterprise problems such as interoperability and information sharing with the intent of improving enterprise performance of mission or business operations.

RECOMMENDED ATTENDANCE

The course is for CIOs and other leaders charged with formulating and guiding the strategic direction of the enterprise. The course has a managerial rather than a technical focus, and is particularly appropriate for middle to senior leaders responsible to the executive management team.

PREREQUISITES

None

LEARNING OUTCOMES

Students will be able to identify problems stemming from the absence of an EA and develop a strategy to use an EA effectively to overcome them; integrate EA with the organization's strategic and resource planning, information assurance, and acquisition management processes; and use a capability maturity framework to evaluate an enterprise's architectural management processes.

ATO

APPROVAL TO OPERATE: INFORMATION SYSTEM CERTIFICATION AND ACCREDITATION

Subject: IRMC-INT
Catalog Number: 6209

COURSE DESCRIPTION

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 Approving Authority (DAA) in approving the classification level of an information system and granting ATO at a specified level of trust. The course provides an overview of DoD and federal department and agency certification and accreditation processes (e.g., Defense Information Technology Security Certification and Accreditation Process; National Information Assurance Certification and Accreditation Process), acquisition management, and system security architecture considerations.

RECOMMENDED ATTENDANCE

This course is appropriate for senior system managers, information system certification and accreditation managers, and program managers who are responsible for participating in the certification and accreditation process for delivery of ATO documentation to the DAA.

PREREQUISITES

None; however, students who have no information assurance background should take Information Assurance and Critical Infrastructure Protection (AII) before taking this course.

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

Subject: IRMC-INT
Catalog Number: 6430

COURSE DESCRIPTION

This course explores the principles, processes, and practices involved in developing, evaluating, and defending information technology (IT) investment business cases. The course stresses the value to the enterprise of the holistic evaluation of IT investment business cases as an element of enterprise transformation. The course emphasizes the components of the Office of Management and Budget (OMB) Circular A-130, Part 7, Section 53, Information Technology and E-Government, and Section 300, Planning, Budgeting, Acquisition, and Management of Capital Assets. It explores best practices and strategies for building a successful federal IT business case, including application of architecture, business process reengineering, capital planning, analysis of alternatives, risk assessments, and information assurance investment. The students use a business case evaluation method and other business case criteria to develop a hypothetical IT business case and to evaluate an IT business case.

RECOMMENDED ATTENDANCE

This course is for leaders and managers who are responsible for developing, analyzing, or defending a business case for IT investments.

PREREQUISITES

None

LEARNING OUTCOMES

Students will be able to critique a business case using a business case evaluation method and other business case criteria, and recommend changes to improve the defense of the business case to OMB and agency officials; and to create a hypothetical IT business case.

CBL

CYBERLAW

Subject: IRMC-INT

Catalog Number: 6204

COURSE DESCRIPTION

The 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.

RECOMMENDED ATTENDANCE

This course is appropriate for senior leaders who must manage organizations that depend upon the information infrastructure. This includes, but is not limited to, federal and military information operators; Chief Information Officers; Chief Information Security Officers; military and federal personnel who develop and manage information resources; and students in Professional Military Education programs (intermediate and senior).

PREREQUISITES

None; however, students who have no information assurance background should take Information Assurance and Critical Infrastructure Protection (AII) before taking this course.

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.

CIP

PROTECTION OF CRITICAL INFRASTRUCTURE AND KEY ASSETS

Subject: IRMC-INT

Catalog Number: 6212

COURSE DESCRIPTION

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.

RECOMMENDED ATTENDANCE

This course is intended for middle to senior managers who are involved in the planning, supporting, and/or execution of missions related to homeland security. It assumes no background in this area. Knowledge of basic computing skills such as web searching is required.

PREREQUISITES

None; however, students may enhance their understanding by taking Homeland Security Information Management (HLS) followed by the Homeland Security Information Management: Tools & Techniques (HST).

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

Subject: IRMC-INT
Catalog Number: 6504

COURSE DESCRIPTION

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.

RECOMMENDED ATTENDANCE

This course is appropriate for all persons who must develop, lead, or collaborate on continuity of operations issues.

PREREQUISITES

None

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

Subject: IRMC-INT
Catalog Number: 6510

COURSE DESCRIPTION

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.

RECOMMENDED ATTENDANCE

This course is appropriate for functional and information resource managers who seek a greater understanding of the current state of the art and the trends in information systems technology. No formal technical background is required.

PREREQUISITES

None

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

Subject: IRMC-INT
Catalog Number: 6317

COURSE DESCRIPTION

This course provides a broad summary of duties of a Chief Information Officer. Using key federal statutes and policy as a backdrop, the course examines both explicit and implicit functions of the CIO. The primary focus is on how laws, as well as current policy and best business practices, should be applied when planning, acquiring, managing, and using information resources. Set in the context of an increasingly dynamic global environment, the course provides a comprehensive examination of information resources management in the federal government with emphasis on its critical role in achieving competitive advantage by improving mission performance and service delivery.

RECOMMENDED ATTENDANCE

The course is appropriate for Chief Information Officers and their staff, as well as individuals with business functional responsibilities associated with the leadership of the information component of national power.

PREREQUISITES

None; however, it is recommended as the first course taken in the CIO Certificate Program.

LEARNING OUTCOMES

Students will be able to develop a program of actions for implementing the requirements of the Clinger-Cohen Act and other related directives and legislation in their organizations.

DBE

DEFENSE BUSINESS ENTERPRISE TRANSFORMATION

Subject: IRMC-INT
Catalog Number: 6501

COURSE DESCRIPTION

This course focuses on initiatives, strategies, and opportunities for transforming the DoD's business operations that provide capabilities, resources, and materiel to the global war-fighter. The course assesses the structural, political, technological, leadership, and human challenges of effecting transformational change in a complex mega-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 Global Information Grid (GIG) 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 DoD business enterprise transformation.

RECOMMENDED ATTENDANCE

The course is critical for DoD officers and civilian executives, and of interest in a comparative sense for other Federal agency officers and civilian executives who hold, or aspire to hold leadership positions with transformation responsibilities.

PREREQUISITES

None

LEARNING OUTCOMES

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

DMS

DATA MANAGEMENT STRATEGIES AND TECHNOLOGIES: A MANAGERIAL PERSPECTIVE

Subject: IRMC-INT
Catalog Number: 6414

COURSE DESCRIPTION

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 the students can evaluate the capabilities and limitations of data management options and strategies.

RECOMMENDED ATTENDANCE

The course is designed for mid- to senior-level managers in both technical and non-technical functions who seek a greater understanding of data management strategies and the state of the art and trends in data technologies.

PREREQUISITES

None; however, students in the Enterprise Architecture Certificate program are encouraged to complete the Information Management Planning (IMP) and Strategies for Process Improvement (PRI) courses before enrolling in DMS.

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.

DTF

DEFENSE TRANSFORMATIONS

Subject: IRMC-INT
Catalog Number: 6509

COURSE DESCRIPTION

This course focuses on transformation initiatives relating to DoD capabilities, forces, and the Enterprise, and collaborative multi-agency national security and coalition arrangements. The course places current DoD transformation efforts within the retrospective of Information Age drivers, examining relevant and current Revolutions in Military and Business Affairs. This is followed by a prospective context examining the innovations in information associated with network centric warfare, operations, and enterprise management concepts. It examines how these innovations in leveraging the information power of networked teams, forces, organizations, and coalitions are being used to deconstruct and reshape the DoD into an agile organization that can adapt swiftly to perform diverse defense, national, and homeland security missions. The course analyzes strategies leaders have adopted to effect DoD transformation, including experimentation and joint capability concepts. The course examines the challenges and opportunities posed for transformation leaders who seek to transform a complex mega-enterprise while simultaneously preparing and leading global war-fighting and peace building operations.

RECOMMENDED ATTENDANCE

The course is critical for DoD, national, and international security community officers and civilian executives, particularly State and Homeland Security Departments, who or aspire to hold leadership positions with transformation responsibilities.

PREREQUISITES

None

LEARNING OUTCOMES

Students will be able to evaluate critically the ends, ways, and means of defense transformation; evaluate the dynamics of challenges posed by and opportunities presented for defense transformation; develop critical competencies for leading transformation initiatives by experimenting with one aspect of DoD's transformation effort; and propose and defend recommendations for alternative transformation approaches and actions.

EAP

ENTERPRISE ARCHITECTURE PRACTICUM

Subject: IRMC-INT

Catalog Number: 6413

COURSE DESCRIPTION

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.

RECOMMENDED ATTENDANCE

This course is intended for leaders and practitioners with current or anticipated responsibilities that involve leading the development or management of an enterprise architecture.

PREREQUISITES

In addition to the following courses, students should have an approved project proposal before enrolling in EAP.

- Information Management Planning (IMP)
- Strategies for Process Improvement (PRI)
- Enterprise Architecture for Managers (ARC)
- Data Management Strategies and Technologies (DMS)
- Planning and Managing Enterprise Architecture Programs (PMA)
- Global Information Grid Architecture and Advanced Concepts (GIG) or Federal Enterprise Architecture and Advanced Concepts (FAC)

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.

EGV

eGOVERNMENT

Subject: IRMC-INT

Catalog Number: 6505

COURSE DESCRIPTION

This course examines the phenomenon and consequences of eGovernment and eGovernance from executive, program, and CIO perspectives. It addresses the growing role of and trend toward infusing information technology into government and governance processes, and examines leadership and managerial challenges posed by eGovernment and boundary-spanning programs and IT initiatives. Governance models, legislation, policies, and current eGovernment programs are investigated. Issues such as dealing with change and integrating performance and budgets across agencies are investigated. This policy-oriented course focuses on assessing the potential of eGovernment, its rationale, and its challenges.

RECOMMENDED ATTENDANCE

The course is designed for executives desiring a greater understanding of the challenges and rewards of electronic government. Intended to provide a broad and integrative view of eGovernment models, initiatives, and approaches, the course provides a policy foundation for assessing the issues attendant to transforming government and governance.

PREREQUISITES

None

LEARNING OUTCOMES

Students will be able to explain the ideas, policies, and programs of eGovernment initiatives; assess the ongoing transformation in governance and its processes; and articulate the leadership and managerial challenges posed by eGovernment policies, technologies, and issues in a democratic society.

ESG

EXPERIMENTATION, SIMULATION, AND GAMING: TESTBED FOR TRANSFORMATION

Subject: IRMC-INT

Catalog Number: 6502

COURSE DESCRIPTION

This course focuses on the strategies, processes, and technologies of experimentation as a key enabler for defense, national, and homeland security transformation efforts. The course examines the role played by experimentation, and lessons learned in evolving the concepts and doctrine of information-enabled network centric warfare and operations, and in informing priorities and choices for investing in future joint, service, and multi-agency capabilities. The course reviews the principles, key methods, collaborative knowledge management, and visualization information technologies being used to conduct effective experiments. The spectrum of experimentation efforts currently ongoing to support defense, national, and homeland security transformation efforts is reviewed.

RECOMMENDED ATTENDANCE

The course is critical for DoD and other National and Homeland security officers and civilian executives, who hold, or aspire to hold, leadership positions with transformation responsibilities.

PREREQUISITES

None

LEARNING OUTCOMES

Students will be able to identify a spectrum of experimentation methods, analyze each, and recommend appropriate methods that will aid the information leader in transforming the agency to meet the mission.

ESS

ENTERPRISE INFORMATION SECURITY AND RISK MANAGEMENT

Subject: IRMC-INT

Catalog Number: 6206

COURSE DESCRIPTION

This course develops the knowledge and competencies required to lead, implement, and manage an organization's information security and risk management program. It examines the practical challenges of managing information security risks and protecting enterprise information and information systems. Based upon OMB, NIST, and DoD risk management guidance, the course addresses the key components of an organization's information security program that addresses the identification, assessment, mitigation, and acceptance of risk. The course builds upon fundamental information assurance concepts and information security technology, integrating them into scalable, practical working solutions for defending the enterprise. Topics include information security risk assessment, program and system security planning, policy, metrics, architecture, and acquisition.

RECOMMENDED ATTENDANCE

This course is appropriate for managers and practitioners who require a practical perspective on the management of an enterprise information assurance program.

PREREQUISITES

None, but it is strongly recommended that students take Information Assurance and Critical Infrastructure Protection (AII), Global Enterprise Networking and Telecommunications (GEN), and Managing Security in a Networked Environment (SEC) before taking this course.

LEARNING OUTCOMES

Students will be able to assess an organization's information security risks and information security posture, recommend information assurance program components, and develop an enterprise risk management strategy.

FAC

FEDERAL ENTERPRISE ARCHITECTURE AND ADVANCED CONCEPTS

Subject: IRMC-INT

Catalog Number: 6409

COURSE DESCRIPTION

This course examines issues involved in determining compliance and application of the Office of Management and Budget's (OMB's) Federal Enterprise Architecture (EA) Reference Models and OMB Circular A-130. The architecture's role in contributing to the success of the agency's mission is examined. Topics include an assessment of techniques to leverage the EA repository to develop business-line strategic strategies; determine the critical success factors for institutionalizing governance processes; examine and interpret GAO and OMB EA management maturity frameworks; determine success strategies for phasing in an EA; and integrate security and privacy requirements. Other topics include the development of business cases and integration of the Information Technology (IT) portfolio budget cycle (i.e., OMB A-11), data management, and interoperability in the Information Age.

RECOMMENDED ATTENDANCE

This course is targeted for civilian leaders and practitioners with current or future responsibilities to oversee development or management of a non-DoD enterprise architecture. DoD personnel should take the corresponding DoD-focused GIG course.

PREREQUISITES

Enterprise Architectures for Managers (ARC)

LEARNING OUTCOMES

Students will be able to evaluate and select enterprise architecture development and implementation strategies that will contribute to the agency's mission; assess whether a proposed investment is consistent with an enterprise architecture and the OMB reference models; and effectively apply governance strategies to sustain the use and integration of an enterprise architecture with an agency's activities.

GEN

GLOBAL ENTERPRISE NETWORKING AND TELECOMMUNICATIONS

Subject: IRMC-INT

Catalog Number: 6205

COURSE DESCRIPTION

This course focuses on the management of network and telecommunications technology in a global networked enterprise. This course examines current and emerging network and telecommunications technologies, including their costs, benefits, security implications, implementation impacts, and various military and civilian network-centric applications. Selected technical and management topics are discussed to include network-centric concepts, spectrum management, local and wide area networks and associated Internet technologies, and the significance of shifts in regulatory and industry structure.

RECOMMENDED ATTENDANCE

The course is appropriate for mid- to senior-level executives in both technical and nontechnical functions who seek a greater understanding of telecommunications and network management technologies. While aimed at managers, sufficient insight is provided to ensure that the students understand the inherent capabilities and limitations of those technologies.

PREREQUISITES

None; however, it is strongly recommended that this course be the second course taken for the NSTISSI No. 4011 certificate.

LEARNING OUTCOMES

Students will be able to evaluate the managerial and policy consequences of adopting telecommunications and network technologies, and to propose an implementation strategy for incorporating an emerging telecommunication technology to support a network-centric strategy.

GIG

GLOBAL INFORMATION GRID ARCHITECTURE AND ADVANCED CONCEPTS

Subject: IRMC-INT
Catalog Number: 6434

COURSE DESCRIPTION

This course examines issues in assessing consistency with DoD's Global Information Grid (GIG) architecture. The GIG architecture facilitates the Department of Defense's (DoD) Net-Centric Operations and Warfare (NCOW) strategy. Following an examination of net-centric concepts, the course considers the scope, development, and management of the GIG architecture; its relationship to the NCOW Reference Model; the structure, scope, and purpose of the NCOW Reference Model; and its utility in guiding the evolution of the GIG Architecture. The course concludes with a consideration of the actual and potential uses of the GIG architecture to include its application in the Joint Capabilities Integration and Development System (JCIDS) and development of capabilities requirements packages.

RECOMMENDED ATTENDANCE

This course is intended for DoD executives/senior managers and practitioners responsible for developing component or agency architectures or assessing their consistency with the DoD Global Information Grid Architecture. Students from other federal agencies should enroll in the Federal Enterprise Architecture and Advanced Concepts (FAC) course.

PREREQUISITES

Enterprise Architectures for Managers (ARC)

LEARNING OUTCOMES

Students will be able to assess whether a DoD agency's enterprise architecture is consistent with the GIG Architecture and NCOW Reference Model and recommend or select development, implementation, sustainment, or governance and governance strategies consistent with DoD architectural policy and direction.

HLS

HOMELAND SECURITY INFORMATION MANAGEMENT

Subject: IRMC-INT
Catalog Number: 6507

COURSE DESCRIPTION

This course examines issues and emerging information management concepts related to the six critical homeland security mission areas: intelligence and warning, border and transportation security, domestic counterterrorism, protecting critical infrastructure, defending against catastrophic terrorism, and emergency preparedness and response. Students analyze information elements of key asset identification, threat and vulnerability analysis, risk assessment and management, and crisis and consequence management, and technologies for their ability to support planning, mitigation, response, recovery, and prediction. Students discuss functions, responsibilities, and policy; the inter-relationship of defense, government-wide, and nongovernmental information systems; and the importance of strategic and contingency planning, systems integration, and sharing of information.

RECOMMENDED ATTENDANCE

This course is intended for middle to senior managers who are involved in the planning, supporting, and/or execution of missions related to homeland security. It assumes no background in this area.

PREREQUISITES

None

LEARNING OUTCOMES

Students will be able to assess areas within their respective organizations that are critical to the management of information for effective homeland security; provide recommendations for setting priorities and allocating homeland security resources; and develop a homeland security information integration and coordination strategy for their organization.

HST

HOMELAND SECURITY INFORMATION MANAGEMENT: TOOLS & TECHNIQUES

Subject: IRMC-INT

Catalog Number: 6503

COURSE DESCRIPTION

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 provides students with “hands-on” exposure to technologies and techniques that support the planning, mitigation, response, recovery, and prediction aspects 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.

RECOMMENDED ATTENDANCE

This course is intended for senior managers who are involved in the planning, supporting, and/or execution of missions related to homeland security. It assumes no background in this area.

PREREQUISITES

None; however, students should be very familiar with the Homeland Security Information Management (HLS) mission areas and with many of the requirements for risk assessment, consequence management, and some of the technologies needed for better information sharing and international cooperation.

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.

ICS

INFORMATION ENGAGEMENT AND STRATEGIC COMMUNICATION

Subject: IRMC-INT

Catalog Number: 6208

COURSE DESCRIPTION

This course provides an intensive examination of the transformational impact of information engagement and the use of strategic communication in public diplomacy and statecraft. The course covers issues such as the conduct of public or virtual diplomacy; international military information; international broadcasting; the Internet; global television; propaganda; psychological operations; the media; information in the global War on Terror; and perception management, all as means to influence decision makers, population groups, and critical audiences. Several recent real-world situations will provide case studies for analysis. The course concludes by exploring how shaping the information environment and effectively employing the information component of power impacts the national security process.

RECOMMENDED ATTENDANCE

This course is appropriate for strategic leaders, military planners, and personnel desiring to explore and analyze strategic issues involving information and national security.

PREREQUISITES

None

LEARNING OUTCOMES

Students will be able to analyze how strategic communication can shape and influence strategic and political events, and how global perceptions can be shaped and influenced by using the new information technologies; synthesize strategies for effectively employing strategic communication to influence critical audiences; and recommend how to apply these strategies to achieve national security objectives.

IMP

INFORMATION MANAGEMENT PLANNING

Subject: IRMC-INT
Catalog Number: 6318

COURSE DESCRIPTION

This course presents an approach to planning that integrates agency strategic planning, performance planning, information management planning, and the agency budget. It examines a comprehensive mission-driven planning framework that combines explicit and implicit planning requirements of current legislation (e.g., Government Performance and Results Act, Paperwork Reduction Act, Clinger-Cohen Act, etc.) and regulations. This course uses a comprehensive framework that integrates agency strategic planning, agency IRM strategic planning, enterprise architecture planning, and information technology capital planning and investment management to link investment in information resources to improved mission performance.

RECOMMENDED ATTENDANCE

This course is appropriate for those seeking to leverage the capabilities of information technology as a means of improving mission performance. It is particularly well suited to those preparing agency strategic plans and performance plans that link investment in IT to strategic goals and objectives.

PREREQUISITES

None

LEARNING OUTCOME

Students will be able to write an agency strategic plan and an agency information management strategic plan that comply with the requirements of current legislation, regulations, and best practices.

IOS

INFORMATION OPERATIONS AND NATIONAL SECURITY IN THE INFORMATION AGE

Subject: IRMC-INT
Catalog Number: 6207

COURSE DESCRIPTION

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.

RECOMMENDED ATTENDANCE

This course is appropriate for strategic leaders, military planners, and personnel desiring to explore and analyze strategic issues involving information and national security.

PREREQUISITES

Secret clearance is required.

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

Subject: IRMC-INT
Catalog Number: 6411

COURSE DESCRIPTION

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.

RECOMMENDED ATTENDANCE

Recommended for leaders and managers with current or anticipated IT program/project leadership responsibilities.

PREREQUISITES

None

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 orally or in writing.

ITA

STRATEGIC INFORMATION TECHNOLOGY ACQUISITION

Subject: IRMC-INT
Catalog Number: 6415

COURSE DESCRIPTION

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. Guest speakers from government and industry round out the course with the latest in policy updates and how to maximize productivity in the contractor-government acquisition environment.

RECOMMENDED ATTENDANCE

This course is appropriate for middle to senior information technology professionals and project leaders seeking a greater understanding of the information technology acquisition process and its relationship to achieving agency strategic business objectives.

PREREQUISITES

None

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

Subject: IRMC-INT
Catalog Number: 6416

COURSE DESCRIPTION

This course focuses on project and program management in an Information Technology (IT) context. In an extensive simulation, students gain hands-on project management experience by performing complex project management tasks leading to the development of a project management strategy/plan. Topics include IT project personnel, scope, integration, cost-schedule-performance, quality, risk, and procurement, as well as the leadership capabilities and strategies needed to manage these aspects of a project. The factors that make large-scale software and other IT programs unique and difficult to manage are explored, along with tools and techniques for managing them. Students also integrate the management reforms mandated by the Clinger-Cohen Act, other legislation, and IT project management best practices into the management of IT programs and projects.

RECOMMENDED ATTENDANCE

This course is for leaders without substantial program/project management experience who expect to assume CIO, program executive office, or other middle- to senior-level responsibilities for program/project oversight. This course requires and assumes familiarity with the IT management reform requirements of the Clinger-Cohen Act of 1996, including IT architecture and requirements management, IT capital planning, and modular contracting.

PREREQUISITES

None; however, successful completion of Strategic Information Technology Acquisition (ITA) is recommended.

LEARNING OUTCOMES

Students will be able to develop a project management strategy/plan for an IT project.

IWS

INFORMATION, WARFARE, AND MILITARY STRATEGY

Subject: IRMC-INT
Catalog Number: 6202

COURSE DESCRIPTION

This course examines key considerations for the planning and conduct of Information Operations (IO) at the theater and strategic levels. The course emphasizes interagency, international, and organizational transformation considerations in the planning and conduct of IO. The course also examines selected non-U.S. approaches to the strategies for, and uses of, the full spectrum of IO 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.

RECOMMENDED ATTENDANCE

This course is appropriate for strategic leaders, military planners, and personnel desiring to explore and analyze strategic issues involving information and national security.

PREREQUISITES

Secret clearance is required.

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.

KMI

KNOWLEDGE MANAGEMENT AND INFORMATION SHARING

Subject: IRMC-INT
Catalog Number: 6506

COURSE DESCRIPTION

This course focuses on how to share organizational information, “connect the dots,” and manage intellectual capital in order to increase organizational effectiveness. The course covers issues related to overcoming barriers to effective information exchange and basic elements of knowledge management such as the role of communities of practice, as well as the technological tools within the field. The course also examines how to improve formal lessons, learned programs and other routes to better corporate information sharing.

RECOMMENDED ATTENDANCE

This course is intended for middle to senior leaders who are seeking to improve information sharing and the use of intellectual capital within their organizations. Familiarity with principles of using information resources as a strategic asset would be useful.

PREREQUISITES

None

LEARNING OUTCOMES

Students will be able to develop effective information sharing strategies; apply knowledge management concepts and develop approaches for measuring and using intellectual capital within their organizations; assess proposals that integrate knowledge management programs with other efforts to improve organizational effectiveness; and evaluate the techniques and technologies available to improve their organization’s management of information and knowledge.

LDC

LEADERSHIP FOR THE INFORMATION AGE

Subject: IRMC-INT
Catalog Number: 6301

COURSE DESCRIPTION

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.

RECOMMENDED ATTENDANCE

The course is for middle- to senior-level managers who lead Information Age organizations.

PREREQUISITES

None

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

LEADING STRATEGIES FOR DISRUPTIVE INNOVATION

Subject: IRMC-INT
Catalog Number: 6511

COURSE DESCRIPTION

This course focuses on the strategies leaders need to create and implement to guide their organizations successfully through disruptive innovations not of their making, as well as to create disruptive innovations necessary to take organizations into new mission spaces. The course reviews catalysts of disruptive innovation to include emerging technology, legislation, globalization, and security. The course identifies leadership risk-taking strategies for creating disruptive innovation. Evolving concepts of enabling and facilitating innovation, experimentation, intelligence gathering, and futures assessments, and developing new competencies designed to cope with disequilibrium, uncertainty, and rapid rates of change are explored. Students evaluate the features of a culture of innovation in organizations, and analyze strategies through which innovation is rewarded, catalyzed, and focused rather than stifled, punished, and dissipated.

RECOMMENDED ATTENDANCE

The course is critical for DoD, national and international security community officers, and civilian executives, particularly State and Homeland Security Departments, who hold or aspire to hold leadership positions with transformation responsibilities.

PREREQUISITES

None

LEARNING OUTCOMES

Students will be able to develop alternative strategies for achieving organizational transformational goals; analyze the benefits and risks of each alternative for the leader and organization; analyze dysfunctional innovative cultures; and create turnaround strategies that enable effective cultures of innovation in their organizations.

MAC

MULTI-AGENCY INFORMATION-ENABLED COLLABORATION

Subject: IRMC-INT
Catalog Number: 6512

COURSE DESCRIPTION

This course focuses on identifying, analyzing, and recommending strategies, means, and information models needed to pursue multi-agency collaboration in support of national and homeland security and national preparedness planning, decision-making, and implementation of plans. It examines current and proposed strategies, means, and models for transforming cross-boundary collaboration and leadership at the federal, state, and local levels, and multilateral collaboration situations with nongovernmental (NGO), media, and international organizations and coalition partners. The course examines how information-enabled networks, collaborative tool-sets, cross-boundary information-sharing and work processes, professional development experiences, and alternative coordination architectures examples can be harnessed in support of effective multi-agency and multi-lateral national and homeland security activities.

RECOMMENDED ATTENDANCE

The course is critical for DoD, national and international security community officers, and civilian executives, particularly State and Homeland Security Departments, who hold or aspire to hold leadership positions with transformation responsibilities.

PREREQUISITES

None

LEARNING OUTCOMES

Students will be able to analyze and recommend strategies, means, and information models needed to pursue transformational multi-agency collaboration in support of national and homeland security and national preparedness planning, decision-making, and implementation; and analyze and recommend the appropriate information-enabled networks, collaborative tool-sets, cross-boundary information-sharing and work processes, professional development, and alternative coordination architectures support to effective multi-agency and multi-lateral national and homeland security activities.

MOP

MEASURING RESULTS OF ORGANIZATIONAL PERFORMANCE

Subject: IRMC-INT
Catalog Number: 6316

COURSE DESCRIPTION

This course provides strategies and techniques for assessing organizational performance results as part of the strategic planning and budgeting process to meet regulatory oversight requirements (e.g., GPRA, Clinger-Cohen Act, President's Management Agenda, PART). The course leverages lessons learned from interagency and private sector experiences on the leadership, process, and resource issues surrounding the identifying, developing, and validating performance measurement instrumentation, collecting and organizing performance data, and analyzing and reporting organizational results. Using the Kaplan and Norton Balanced Scorecard methodology, organizational performance measures are developed that tie to the organizational mission, vision, goals, objectives, initiatives, budget, strategy, and outcomes. A priority emphasis is placed on organizational outcomes as those outcomes link mission accomplishment to value added to the customer.

RECOMMENDED ATTENDANCE

This course is designed for strategic leaders in all career tracks. It is conceptual, not technical, and requires no prior knowledge of performance assessment.

PREREQUISITES

None; however, it is recommended as one of the first two courses taken in the CIO Certificate Program.

LEARNING OUTCOMES

Students will be able to develop and/or assess a comprehensive plan for conducting a performance assessment in their organization that can aid decision makers in leading their organization toward mission effectiveness.

MTI

INFORMATION TECHNOLOGY CAPITAL PLANNING

Subject: IRMC-INT
Catalog Number: 6315

COURSE DESCRIPTION

This course focuses on state-of-the-art strategies for IT Capital Planning, with an emphasis on assessing and managing information technology (IT) as a portfolio of investments. The three phases of the IT investment management process are considered: selection, control, and evaluation of proposals; ongoing projects; and existing systems. The relationship of IT performance measures to mission performance measures is explored. The course examines the roles of the CIO and other managers in developing IT assessment criteria and considers how the criteria are used in planning and managing the IT portfolio. Individual and team exercises are employed, including a simulation of the operation of the Investment Review Board.

RECOMMENDED ATTENDANCE

This course is appropriate for persons preparing agency strategic plans and performance plans that link investment in IT to strategic goals and objectives.

PREREQUISITES

None; however, it is recommended as one of the last courses students should complete in the CIO Certificate Program.

LEARNING OUTCOMES

Students will be able to evaluate an information technology capital planning and investment management process to ensure that it complies with current statutes and regulations, recommend changes to the process, and develop a strategy for balancing a portfolio of IT projects.

NCW

NETWORK CENTRIC WARFARE AND OPERATIONS

Subject: IRMC-INT
Catalog Number: 6513

COURSE DESCRIPTION

This course examines the key tenets and technologies of network centric warfare and operations (NCW) as an evolving way of warfare and a central component of DoD transformation efforts. The nature and dynamics of information-enabled networks underpinning NCW and the emerging information and technologies that could influence how NCW evolves are examined. The impact and performance opportunities presented by such networks and networking in traditional combat and non-traditional combat operations are evaluated using examples of performance advances in information fusion, individual and unit/formation-level situational awareness, and self-synchronization of effort and effect from operations in Kosovo, Iraq, Afghanistan, and from Service, Joint, and multi-national exercises, experiments, demonstrations, and case studies. The course examines NCW-type mission capability packages in terms of leadership and doctrine; command, control, and operational processes; organizational structures, information, and knowledge management approaches, personnel, material, and infrastructure resourcing; and investment decisions and plans. The course examines aspects of the transformation strategy that are being applied through which NCW as an evolving way of war is being created, evolved, and disseminated.

RECOMMENDED ATTENDANCE

The course is critical for DoD, national and international security community officers (particularly from the NATO Alliance and other coalition partners) who hold or aspire to hold leadership positions with transformation responsibilities.

PREREQUISITES

None

LEARNING OUTCOMES

Students will be able to construct, evaluate and recommend appropriate NCW principles, approaches, and technologies to affect requisite transformational change in strategic, operational planning, non-traditional combat planning, and doctrine development efforts.

PMA

PLANNING AND MANAGING ENTERPRISE ARCHITECTURE PROGRAMS

Subject: IRMC-INT
Catalog Number: 6432

COURSE DESCRIPTION

This course provides practical experience in creating enterprise architecture plans and products from a management perspective. Hands-on exercises implementing the DoD Architecture Framework (DoDAF) challenge managers to think critically about how to put theory into practice. These exercises include developing an enterprise architecture project plan and using tools to create and explore DoDAF architecture products. The course also explores how to use enterprise architecture to analyze operational or business requirements and capabilities, identify optimal solutions, and determine transition strategies.

RECOMMENDED ATTENDANCE

The course is for middle to senior IT personnel and managers responsible for leading or overseeing enterprise architecture programs and projects.

PREREQUISITES

Enterprise Architectures for Managers (ARC)

LEARNING OUTCOMES

Students will be able to develop an effective plan for an enterprise architecture project; select and create DoD architecture views and products to satisfy an enterprise architecture project's purpose and scope; and apply enterprise architecture products to analyze operational or business requirements and capabilities, identify optimal solutions, and determine transition strategies.

PRI

STRATEGIES FOR PROCESS IMPROVEMENT

Subject: IRMC-INT

Catalog Number: 6333

COURSE DESCRIPTION

This course examines strategies, management processes, and resources for process improvement within and across federal agencies. It contrasts discontinuous, automation-focused business process re-engineering with the expanding focus on continuous-process customization and managed improvement. An executive-level perspective is provided on the tools, techniques (for example, benchmarking, quality improvement programs, activity-based costing), and technologies that enable process-centric performance improvements to achieve agency missions. The course also contrasts the Industrial Age function-centric enterprise with the Information Age process-centric enterprise and broader process-centric partnerships, networks, coalitions, and alliances. Attention is given to the leadership challenges of initiation, collaboration, design, implementation, and portfolio project management of process-centric improvements within and across agencies.

RECOMMENDED ATTENDANCE

The course is particularly valuable for managers with current or future responsibilities for managing organizational and process improvement within agencies and between agency/enterprise partners. Executives who are responsible for providing strategic leadership for agency-centric process innovation and for collaboration in cross-agency process improvement initiatives and networked process work will also find this course valuable.

PREREQUISITES

None

LEARNING OUTCOMES

Students will be able to recommend appropriate process change strategies, tools, and methods for carrying out agency-centric and cross-agency process improvement; and design and propose strategies for addressing implementation challenges of process improvement, including impacts upon organizational culture, structure, and governance.

SAA

STRATEGIC MANAGEMENT OF SOFTWARE ASSURANCE

Subject: IRMC-INT

Catalog Number: 6211

COURSE DESCRIPTION

This course explores national security issues and leadership responsibilities involved in assuring the safety and security of the software component of the critical information infrastructure. It examines “building security in” to avoid software vulnerabilities that open mission-critical or national security systems to cyber attacks or terrorism. The course explores leveraging the acquisition process to implement safer and more secure software. Other topics include information assurance vis-à-vis software assurance; software assurance (SwA)-related law and public policy; national initiatives sponsored by DHS and DoD; risk management; acquisition issues: offshore development, software pedigree, and strategies for COTS, development and integration services; education, training and the SA Body of Knowledge; and assurance cases.

RECOMMENDED ATTENDANCE

This course is appropriate for middle to senior leaders who are responsible for the management, acquisition, or development of business, mission-critical, or national security systems.

PREREQUISITES

None

LEARNING OUTCOMES

Students will be able to analyze law, public policy, and national security initiatives and to develop an enterprise software assurance leadership plan (involving people, processes, techniques, and technologies) to improve safety and security of software.

SAL

SOFTWARE ACQUISITION LEADERSHIP

Subject: IRMC-INT

Catalog Number: 6410

COURSE DESCRIPTION

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.

RECOMMENDED ATTENDANCE

This course is recommended for middle to senior leaders and managers responsible for leading or overseeing software acquisition, integration, or development projects.

PREREQUISITES

None; however, prior successful completion of Strategies for Process Improvement (PRI) is encouraged.

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.

SCS

MANAGING SECURITY OF CONTROL SYSTEMS

Subject: IRMC-INT

Catalog Number: 6210

COURSE DESCRIPTION

SCS 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 peculiar 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 base-level continuity of operations. The move toward integration of CS with traditional computer networks is covered.

RECOMMENDED ATTENDANCE

This course is appropriate for functional and technical managers who require a foundation in threats to basic control systems infrastructure and to emerging methods for countering those threats.

PREREQUISITES

None

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

MANAGING INFORMATION SECURITY IN A NETWORKED ENVIRONMENT

Subject: IRMC-INT

Catalog Number: 6201

COURSE DESCRIPTION

This course provides a “Defense in Depth” perspective on protecting computer-based information in a modern networked environment. The course covers a wide range of technical issues and topics including Information Assurance Technical Framework (IATF) as a security posture evaluation guideline; basics of network security; firewalls and intrusion detection; transmission security and TEMPEST; threats, vulnerabilities, and risks; network vulnerability assessment; operating system security; web security; encryption, key management, and PKI; physical and personnel security; incident handling and forensics; authentication, access control, and biometrics; wireless security; and emerging network security technologies. The course also defines the role of all personnel in promoting security awareness.

RECOMMENDED ATTENDANCE

This course is appropriate for functional and technical managers who require a foundation in the threats to security of information in a networked environment and emerging methods for countering those threats.

PREREQUISITES

None; however, it is strongly recommended that students take Information Assurance and Critical Infrastructure Protection (AII) and Global Enterprise Networking and Telecommunications (GEN) before taking this course.

LEARNING OUTCOMES

Students will be able to evaluate the network security posture of an organization using the IATF to determine adequate people, process, and technology security.

SPA

PRIVACY RIGHTS AND CHALLENGES IN THE INFORMATION AGE

Subject: IRMC-INT

Catalog Number: 6508

COURSE DESCRIPTION

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. Managers learn to deal with the privacy concerns of citizens and stakeholders when implementing new systems and technology and transforming agency processes. Topics include an examination of the rights, needs, and perspective of the citizen, and the policy and legal frameworks of privacy. Mechanisms for evaluating and dealing with privacy issues are covered, including producing Privacy Impact Assessments (PIAs) for system initiatives and designating Chief Privacy Officers. The course culminates in an examination of leadership and management approaches that ensure appropriate information access and privacy protection.

RECOMMENDED ATTENDANCE

The course is particularly valuable for managers with current or future responsibilities dealing with privacy, the processing of private information, or cross-agency information sharing. This is a non-technical course, and requires no prior knowledge of information privacy.

PREREQUISITES

None

LEARNING OUTCOMES

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

TRANSFORMATION AS STRATEGIC ALIGNMENT

Subject: IRMC-INT
Catalog Number: 6528

COURSE DESCRIPTION

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, in order 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.

RECOMMENDED ATTENDANCE

The course is critical for DoD, national and international security community officers and civilian executives, particularly State and Homeland Security Departments, who hold or aspire to hold leadership positions with transformation responsibilities.

PREREQUISITES

None

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.

ACADEMIC PARTNERSHIP PROGRAM



The IRM College has academic partnerships with universities and colleges across the United States. Graduates from one or more of the IRM College’s certificates can apply to a number of partner institutions toward completion of a master’s or doctoral degree program at the partner school. Partner institutions will accept between 9 and 15 graduate credits depending on which certificate program a student completed at the IRM College. Academic partners provide full-time, part-time, and distributed learning (DL) opportunities. Availability of DL and part-time programs varies by university.

IRM College partner institutions, website addresses, e-mail addresses, applicable degree programs, and points of contact are listed in the table below. The website of each partner institution provides general information on its degree programs; however, you should contact the representative listed below for specific details relating to acceptance of the IRM College courses and admission requirements for IRM College graduates. Individuals participating in the DoD Information Assurance Scholarship Program (IASP) may select only those programs annotated with “IASP qualified.”

The IRM College actively seeks to develop new academic partnerships based on strategic requirements. Check the IRM College website for the most current version of this listing ([http://www.ndu.edu/IRM College/partnerships](http://www.ndu.edu/IRM_College/partnerships)). Contact Ms. Patty Coopersmith (coopersmithp@ndu.edu) or Dr. Brenda Roth (rothb@ndu.edu) for more information.

IRM College Partner	
University	Degrees Available per Partnership Agreement
Auburn University (AL) Samuel Ginn College of Engineering John “Drew” Hamilton hamilton@eng.auburn.edu 334-844-6360	<u>Master of Software Engineering</u> (Additional 24 credits required; some online courses available.) (IASP qualified.) 9 credit hours for IA 4011 Certificate graduates.
Capitol College (MD) Graduate School Ken Crockett ken@capitol-college.edu 301-369-2800, ext. 3025	<u>Master of Science in Information and Telecommunications Systems Management (ITSM)</u> (37-38 credit hours; traditional and/or online classes; credit hours applied to specific courses.) 15 credit hours accepted for AMP graduates or CIO Certificate graduates.

<p>East Carolina University (NC) School of Industry and Technology</p> <p>Biwu Yang yangb@mail.ecu.edu 252-328-9666</p>	<p><u>Master of Science in Industrial Technology (MSIT)</u> (Concentration in Digital Communication, Computer Networking Management, or Information Security.) (36 credit hours; credit hours applied to specific courses; courses available online.) (IASP qualified.)</p> <p>15 credit hours accepted for AMP graduates or CIO Certificate graduates; or 9 credit hours for IA 4011 Certificate graduates.</p>
<p>Eastern Michigan University (MI) College of Technology, School of Technology Studies</p> <p>Gerald "Skip" Lawver Skip.lawver@emich.edu 734-487-1590</p>	<p><u>Masters of Liberal Studies (Concentration in Information Assurance.)</u> (Additional 15 to 21 credit hours required.)</p> <p>15 credits for CIO Certificate graduates; or 9 credit hours for IA 4011 Certificate graduates.</p>
<p>George Mason University (VA) School of Public Policy</p> <p>Leslie Metzger-Levin lmetzger@gmu.edu 703-993-8099</p>	<p><u>Master of Arts in New Professional Studies: Knowledge Management</u> (36 credit hours.)</p> <p>15 credit hours accepted for AMP graduates or CIO Certificate graduates.</p>
<p>George Mason University (VA) School of Information Technology & Engineering</p> <p>Stephen Nash snash@gmu.edu 703-993-1499</p>	<p><u>Master of Science in Information Security and Assurance (MSIS)</u> <u>Master of Science in Information Systems (MSIS)</u> <u>Master of Science in Software Engineering (Master of Science-SWE)</u> (All 30 credit hours, all IASP qualified.) <u>Doctorate of Philosophy in Information Technology</u> <u>Doctorate of Philosophy in Computer Science</u> <u>Doctoral Degree Engineer in Information Technology</u> (Number of credit hours for Ph.D. depends on master's degree transferred; credit hours applied toward specific courses.) (All IASP qualified.)</p> <p>9 credit hours accepted for IA 4011 Certificate graduates.</p> <hr style="border-top: 1px dashed black;"/> <p><u>Master of Science in Telecommunications</u> (30 credit hours; credits applied toward specific courses.)</p> <p>9 credit hours accepted for IA 4011 Certificate graduates.</p>

<p>Georgia Institute of Technology (GA) Sam Nunn School of International Affairs & Ivan Allen College of Liberal Arts</p> <p>Seymour “Sy” Goodman Goodman@cc.gatech.edu 404-385-2271</p>	<p><u>Master of Science in International Affairs</u> (IASP qualified.)</p> <p>9 credit hours accepted for IA 4011 Certificate graduates.</p>
<p>James Madison University (VA) College of Graduate and Professional Programs</p> <p>Kenneth Bahn bahnkd@jmu.edu 540-568-3009</p>	<p><u>Master of Business Administration (Concentration in Information Security.)</u> (45 credit hours; credits applied toward specific courses; primarily online.) (IASP qualified.)</p> <p>15 credit hours accepted for AMP graduates or CIO Certificate graduates (with IA 4011 certification); or</p> <p>9 credit hours accepted for IA 4011 Certificate graduates.</p>
<p>James Madison University (VA) Department of Computer Science</p> <p>Hossain Heydari heydarmh@jmu.edu 540-568-8745</p>	<p><u>Master of Science in Computer Science (concentration in Information Security)</u> (33 credit hours; credits applied towards specific courses; cohort distance learning.) (IASP qualified.)</p> <p>9 credit hours accepted for IA 4011 Certificate graduates.</p>
<p>Johns Hopkins University (MD) Information Security Institute</p> <p>Dr. Gerald Masson masson@jhu.edu 410-516-4250</p>	<p><u>Master of Science in Security Informatics (MSSI)</u> (30 hours; credits applied to specific courses.) (IASP qualified.)</p> <p>9 credit hours accepted for IA 4011 Certificate graduates.</p>
<p>Mississippi State University (Master of Science) Bagley College Of Engineering</p>	<p><u>Master of Science in Computer Science (MSC)</u> (20 credit hours required beyond transfer; some courses available online, one year residence required.)</p> <p><u>Ph.D. in Computer Science</u> (Additional 28 hours of coursework and 20 hours dissertation research.) (Both IASP qualified.)</p> <p>15 credit hours for AMP graduates or CIO Certificate graduates (with IA 4011 Certification); or</p> <p>9 credit hours for IA 4011 Certificate graduates only.</p>

<p>Mississippi State University (Master of Science) College of Business and Industry</p> <p>Dave Dampier dampier@CSE.MsState.edu 662-325-8923</p>	<p><u>Master of Science in Information Systems (MSIS)</u> (15 credit hours required beyond transfer; credit applied to specific courses.) <u>MBA in Project Management</u> (Additional 23 hours.) <u>Ph.D. in Business Administration</u> (Major in Information Systems.) (Additional 39 hours required.) (All degrees IASP qualified.)</p> <p>15 graduate credit hours accepted for AMP graduates or CIO Certificate graduates.</p>
<p>New Mexico Tech (NM) Department of Computer Science</p> <p>Dr. Andrew H. Sung sung@cs.nmt.edu 505-835-5126</p>	<p><u>Doctorate of Philosophy in Computer Science</u> (36-42 hours additional required.) (IASP qualified.)</p> <p>9 credit hours accepted for IA 4011 Certificate graduates; or 15 credit hours accepted for CIO Certificate graduates.</p>
<p>Northeastern University (MA) Colleges of Computer and Information Science and College of Criminal Justice</p> <p>Agnes Chan ahchan@ccs.neu.edu 617-373-2464</p>	<p><u>Master of Information Assurance</u> (Additional 24 credits required.)</p> <p>9 credit hours accepted for IA 4011 Certificate graduates.</p>
<p>Northeastern University (MA) School of Professional and Continuing Studies</p> <p>Todd Leach tleach@neu.edu 617-373-2420</p>	<p><u>Master of Professional Studies in Informatics</u> (Additional 20 to 28 quarter hours required.) (IASP qualified.)</p> <p>9 credit hours accepted for IA 4011 Certificate graduates; or 15 credit hours for CIO Certificate graduates.</p> <p><u>Master of Science in Leadership</u> (Additional 21 quarter hours required.)</p> <p>15 credit hours accepted for Organizational Transformation (OT) Certificate graduates.</p>
<p>Pace University (NY) School of Computer Science and Information Systems</p> <p>Bernice Houle bhoule@pace.edu 914-773-3592</p>	<p><u>Master of Science in Internet Technology</u> <u>Master of Science Computer Science</u> <u>Master of Science Information Systems</u> (Additional 21 credit hours for CIO certificate holders; additional 27 credit hours for IA certificate holders.)</p> <p>15 credit hours for CIO Certificate graduates; or 9 credit hours for IA 4011 Certificate graduates.</p>

<p>Polytechnic University (NY) Computer Science Department</p> <p>Nasir Memon memon@poly.edu 718-260-3970</p>	<p><u>Master of Science Computer Science</u> (Additional 27 credits required.)</p> <p>9 credit hours accepted for IA 4011 Certificate graduates.</p>
<p>Regis University (CO) School of Professional Studies</p> <p>Donald Archer archer@regis.edu 303-458-4335</p>	<p><u>Master of Science Computer Information Technology</u> (Additional 21 credits required.)</p> <p>15 credit hours accepted for CIO Certificate graduates, AMP graduates, or Organizational Transformation (OT) Certificate graduates.</p>
<p>Syracuse University (DC, NY) School of Information Studies</p> <p>Scott Bernard sabernar@syr.edu 703-532-4243</p> <p>Kathy Allen kallen02@syr.edu 315-443-4251</p>	<p><u>Master of Science in Information Resource Management (Concentration in Information Assurance or Enterprise Architecture.)</u> (30 credit hours; courses available at the Washington, D.C. campus, online, or at the Syracuse, NY campus.) (IASP qualified.)</p> <p>15 credit hours accepted for AMP graduates or CIO Certificate graduates; or</p> <p>12 credit hours for Enterprise Architecture (EA) graduates; or</p> <p>9 credit hours for IA 4011 Certificate graduates.</p>
<p>Texas A&M University (TX) Center for Information Assurance and Security</p> <p>Wei Zhao w-zhao@tamu.edu 979-845-9776</p>	<p><u>Master of Science Computer Science</u> <u>Master of Science Computer Engineering</u> <u>Master of Computer Science</u> <u>Master of Engineering in Computer Engineering</u> <u>Ph.D. in Computer Science</u> <u>Ph.D. in Computer Engineering</u> <u>Master of Science Electrical Engineering</u> <u>Master of Engineering in Electrical Engineering</u> <u>Ph.D. in Electrical Engineering</u> <u>Master of Science in Management and Information Systems</u> <u>Ph.D. in Information and Operations Management</u></p> <p>21-24 credits additional for Master's; 52 hours for Ph.D. if Master's was in an approved program; 84 if Master's was not in a related field.) (All degrees IASP qualified.)</p> <p>9 credits accepted for IA 4011 Certificate graduates (possibly more credits for those students who complete the CIO Certificate with the IA 4011 certification).</p>

<p>Towson University (MD)</p> <p>Patricia Beere pbeere@towson.edu 410-704-5055</p>	<p><u>Master of Science in Applied Information Technology</u> (33 hours; credits applied to specific courses.) (IASP qualified.)</p> <p>15 credit hours accepted for AMP graduates or CIO Certificate graduates (with IA 4011 certification); or</p> <p>12 credit hours for students with both IA 4011 and 4012 Certificates; or</p> <p>9 credit hours for IA 4011 Certificate graduates.</p>
<p>University of Dallas (TX) Graduate School of Management</p> <p>Mihir Mistry mmistry@gsm.udallas.edu 972-721-4091</p>	<p><u>Master of Business Administration, concentration in Information Assurance</u> (MBA/IS) (49 hours; courses available online; credit hours applied to specific courses.) (IASP qualified.)</p> <p><u>Master of Management in Information Assurance</u> (31 hours; courses available on-line.) (IASP qualified.)</p> <p><u>Master of Science in Information Assurance</u> (31 hours; courses available on-line.) (IASP qualified.)</p> <p>15 credit hours accepted for AMP graduates or CIO Certificate graduates; or</p> <p>9 credit hours for IA 4011 Certificate graduates.</p>
<p>University of Detroit Mercy (MI) College of Business Administration</p> <p>Dan Shoemaker dshoemaker1@twmi.rr.com 313-993-1170</p>	<p><u>Master of Science in IA</u></p> <p><u>Master of Science in Computer and Information Systems</u></p> <p>9 credits for IA 4011 Certificate graduates;</p> <p>12 credits for students with both IA 4011 and IA 4012 Certificates; or</p> <p>15 credits for CIO Certificate graduates (with IA 4011 certification); or</p> <p>15 credits for CISO Certificate graduates.</p>
<p>University of Illinois at Urbana-Champaign (IL) Department of Computer Science</p> <p>Mehdi Harandi Harandi@cs.uiuc.edu 217-333-6952</p>	<p><u>Master of Computer Science</u></p> <p><u>Master of Science in Computer Science</u></p> <p><u>Master of Science in Bioinformatics</u></p> <p>9 credit hours accepted for IA 4011 Certificate graduates.</p>

<p>University of Maryland, Baltimore County (MD) The Graduate School and College of Engineering</p> <p>Alan Sherman dralansherman@starpower.net 410-455-2666</p>	<p><u>Master of Science in Computer Science</u> (30-33 credit hours; resident only.) (IASP qualified.) <u>Master of Science in Computer Engineering</u> (IASP qualified.)</p> <p>9 credit hours accepted for IA 4011 Certificate graduates.</p>
<p>University of Maryland University College (MD) Graduate School of Management & Technology</p> <p>Paul Keller pkeller@umuc.edu 301-985-4616</p> <p>Jim Cronin jcronin@umuc.edu 240-684-5153</p>	<p><u>Master of Science in Computer Systems Management (CSMN)</u> (36-39 credit hours.) <u>Master of Science in Telecommunications Management (TLMN)</u> (36-39 credit hours.) <u>Master of Science in Information Technology (MSIT)</u> (All degrees above have courses available online; credit hours applied to specific courses) (IASP qualified.)</p> <p>15 credit hours accepted for AMP graduates or CIO Certificate graduates.</p>
<p>Robert Ouellette rouellette@umuc.edu 301-985-7833</p>	<p><u>Master of Science in Electronic Commerce</u> (Credits applied to specific courses.)</p> <p>15 credit hours for Organizational Transformation (OT) or eGovernment Certificate graduates.</p>
<p>University of Nebraska at Omaha (NE) The College of Information Science and Technology</p> <p>Blaine Burnham bburnham@mail.unomaha.edu 402-554-2039</p>	<p><u>Master of Science in Management Information Systems (IA concentration)</u> (IASP qualified.)</p> <p>15 credit hours for AMP graduates or CIO Certificate graduates (who also earned IA 4011 certification.)</p> <p><i>(Note: Specific IRM College courses are required for the credit acceptance: CWC, LDC, and DMS.)</i></p>
<p>University of North Carolina at Charlotte (NC)</p> <p>Bill Chu billchu@uncc.edu 704-687-4568</p>	<p><u>Master of Science in Information Technology (MSIT)</u> (30 credit hours; residence only.) (IASP qualified.)</p> <p>15 credit hours for AMP graduates or CIO Certificate graduates (who also earned IA 4011 Certification); or</p> <p>9 credit hours for IA 4011 Certificate graduates.</p>

<p>University of Pittsburgh (PA) Department of Information Sciences and Telecommunications</p> <p>James Joshi jjoshi@mail.sis.pitt.edu 412-624-9982</p>	<p><u>Master of Science in Information Science (MSIS)</u> <u>Master of Science in Telecommunications and Networking (MST&N)</u> (Additional 21 to 27 credits required.) (Both IASP qualified.)</p> <p>15 credit hours for AMP graduates or CIO Certificate graduates (who also earned IA 4011 concentration); or</p> <p>9 credit hours for IA 4011 Certificate graduates.</p>
<p>University of Texas at San Antonio (TX)</p> <p>Glen Dietrich gdietrich@utsa.edu 210-458-5354</p>	<p><u>Master of Science in Information Technology (concentration in Information Assurance)</u> (33 credit hours.) (IASP qualified.)</p> <p>15 credit hours for AMP graduates or CIO Certificate graduates (who also earned IA 4011 certification); <i>(Note: The following IRM College courses are required for the 15 credits to be accepted: LDC, PRI);</i> or</p> <p>9 credit hours for IA 4011 Certificate graduates.</p>
<p>University of Tulsa (OK) Center of Information Security</p> <p>Sujeet Shenoj sujeet@utulsa.edu 918-631-3269</p>	<p><u>Master of Science in Computer Science (Concentration in Information Assurance)</u> (30 credit hours; credit hours applied to specific courses; residence only.) (IASP qualified.)</p> <p><u>Doctorate of Philosophy in Computer Science (concentration in Information Assurance)</u> (90 credit hours, which includes 30 credit hours for transfer of master's degree; 45 additional credit hours needed, if prerequisites are met; credit hours applied to specific courses; residence only.) (IASP qualified.)</p> <p>15 credit hours for AMP graduates or CIO Certificate graduates; or</p> <p>9 credits for IA 4011 Certificate graduates.</p>



SENIOR LEADERSHIP

ROBERT D. CHILDS, 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.

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 and Learning; 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.

MARY L. POLYDYS, Chair, Information Operations and Assurance Department; B.S., M.S.I.S., George Mason University.

CHARLES E. TOMPKINS III, Chair, Systems Management Department; B.A., University of Oklahoma; M.P.A., University of Oklahoma; U.S. Army Command and General Staff College, Defense Systems Management College; J.D., Oklahoma City University.

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

FACULTY

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

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

ANTHONY W. BUENGER, JR., Lieutenant Colonel, USAF, Information Operations and Assurance Department; B.S., University of Maryland; M.A., Webster University.

JUDITH CARR, Information Strategies Department; B.A., M.S., Central Washington University; M.A., Ph.D., The Fielding Institute.

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; J.D., Georgetown University Law Center.

AI-MEI CHANG, Systems Management Department; B.S., Ph.D., Purdue University.

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

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

CARL J. CLAVADETSCHER, Systems Management Department; B.S., Montana State University; M.S., Southern Illinois University; M.B.A., The University of Puget Sound; M.S.-MIS, The Claremont Graduate School; Ph.D., University of Oregon; Post-Doctoral Fellowship, Indiana University.

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

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

JOHN J. DOLAC, Colonel, USA, Information Strategies Department; B.A., Iowa State College; M.A., Webster University.

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

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

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

PAUL H. FLANAGAN, Systems Management Department; A.A., Richard Bland College; B.S., Virginia Commonwealth University; M.A., University of Maryland.

PETER FRANKS, Lieutenant Commander, Royal Navy, Information Strategies Department; BSc., Nottingham University, (United Kingdom); MSc., Southampton Institute, (United Kingdom).

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

DENNIS HALL, Robbins-Gioia Visiting Faculty, Systems Management Department; BS-EE, University of Illinois; MS-EE, University of Illinois; MSA-IRM, George Washington University.

KAREN F. HOGAN, U.S. Department of Commerce Visiting Faculty, Systems Management Department; B.S., Madison College; M.S., The George Washington University.

PHILIP A. IRISH III, Information Strategies Department; B.S., U.S. Air Force Academy; M.A. Ed., Arizona State University; Air Command and Staff College; Defense Systems Management College; Ph.D., The Pennsylvania State University.

MARWAN M. JAMAL, Information Operations and Assurance Department; B.S., M.S., 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.

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.

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

MARK McGIBBON, Lockheed Martin Visiting Faculty, Systems Management Department; B.S., University of Utah; M.S.-ITM, Naval Postgraduate School.

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 Management Department; B.S., University of Maryland; M.S., The American University.

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

LESLIE M. PANG, Systems Management Department; B.S., University of Hawaii; M.S., University of Nebraska; M.B.A., University of Maryland; Ph.D., University of Utah.

RANSON J. RICKS, Lieutenant Colonel, USA, Systems Management Department; B.S., Savannah State University; Master of Engineering Management, Saint Martin's University; M.S., Air University.

ANGELO RIDDICK, 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.

JANICE L. WILEY, Information Strategies Department; B.M., University of Wyoming; M.M., M.Ed., Colorado State University; U.S. Marine Corps Command and Staff College; M.S., Industrial College of the Armed Forces; J.D., University of Wyoming.

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



2006 NDU Volleyball Champions

INFORMATION RESOURCES MANAGEMENT COLLEGE



ADVANCED
MANAGEMENT
PROGRAM

CIO

CHIEF
INFORMATION
OFFICER



ENTERPRISE
ARCHITECTURE



INFORMATION
ASSURANCE



INFORMATION
TECHNOLOGY
PROJECT
MANAGEMENT



ORGANIZATIONAL
TRANSFORMATION



IRM COLLEGE
NATIONAL DEFENSE UNIVERSITY
300 5TH AVE, BLDG 62
FORT MCNAIR, DC 20319
202.685.6300

WWW.NDU.EDU/IRMC



NATIONAL DEFENSE UNIVERSITY