

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

1988

*Twenty Years of Shaping the Future*

2008



Information Resources Management College

2007 - 2008  
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

Senior 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

	<b>6300</b>
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 5<sup>th</sup> Avenue  
Fort McNair, D.C. 20319-5066

**Catalog is current as of 21 May, 2007.**  
**Updates are made on the IRMC website at**  
**[www.ndu.edu/irmc](http://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 (IT-PM) Certificate .....	22
Organizational Transformation (OT) Certificate .....	23
Professional Development Opportunities .....	25

### **Student Services and Policies**

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

<b>Course Descriptions</b> .....	35
----------------------------------	----

<b>Academic Partnership Program</b> .....	58
---	----

<b>Administration and Faculty</b> .....	66
---	----

## MISSION

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



## VISION

The recognized world leader in information resources management education.

## GOALS

- Foster critical thinking and leadership through high-quality graduate-level executive education, development, and scholarship in defense, Joint Professional Military Education, and interagency 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 in both the curriculum and the facilitation of learning
- Nurture and expand strategic partnerships and interactions with the Department of Defense and other government agencies, private sector, academia, and international organizations to enhance learning opportunities for global unity of effort that anticipates and addresses complex security challenges.
- Continually invest in faculty and staff intellectual capital to promote excellence and leadership in IRM education, scholarship, student learning, outreach, and Joint Professional Military Education.
- Leverage information technologies to strengthen college administration and to increase educational services for students and foster lifelong learning in global defense and interagency government communities.



The IRM College is approaching a milestone in 2008! We are proud to be marking our 20th anniversary in educating our nation's information leaders. We grew from a small IT school focused on technology and its applied uses in 1988, to a world-class graduate college offering an array of programs with national and international influence. Throughout the established academic year, we will be offering a series of activities leading up to our anniversary celebration in September 2008. Our students, past and present, represent a vast learning community around the world in such places as Poland, Singapore, Korea, Iraq, Afghanistan, and Kuwait. The College now offers more than 250 courses in Chief Information Officer competencies, Information Assurance, Organizational Transformation, Acquisition, Enterprise Architecture, IT Project Management, and Information Operations. As evidence of the College's global delivery format, nearly 1,000 students completed online (distributed learning) courses in academic year 2006/2007. We look forward to creating and uniting the information community to advance national security in the 21st century.

Our programs are not just for leaders in information technology arenas. The IRM College graduate-level certificate programs develop strategic leaders in all critical areas of national security. Our challenging programs, offered in residence and over the Internet, meet the needs of a diverse and vital government workforce regardless of career field. We foster interagency collaboration and communication by providing learning opportunities for individuals across government. Our international and global U.S. faculty have extensive experiences in government agencies, the Department of Defense, the private sector, and higher education, and they stay connected to bring the latest innovations and issues from the field.

The IRM College is recognized for its academic excellence. We partner with over 30 universities and colleges across the country to provide our graduates with opportunities to complete masters or doctoral degrees. Graduates may apply 9 to 15 credits at a partner institution toward completion of select advanced degree programs. Our certificates lay a strong foundation in important information and information resources management topics and issues to develop strategic leaders for the Information Age.

I am proud of our programs and our international and global faculty. We welcome current students and alumni as members of our growing international community of learners. Now, more than ever, our country needs leaders who can effectively develop, organize, manage, leverage, and protect the country's various information resources to transform government. Please join us as we continue to be at the forefront of issues, concepts, and communities that leverage the information component of national power.

*Robert D. Childs*  
Senior Director, IRM College



*"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*

## **A Global Community of Information Leaders**

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. In addition to graduate-level courses, the IRM College offers all courses for professional development and welcomes students to enroll without seeking a certificate or academic credit. A third option for strategic leader development is "education in context." These educational opportunities include workshops, presentations, forums, and events to develop the government workforce to meet the needs of agencies to accomplish their missions and to develop leaders who can leverage the information component for national security.

## **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.

## Access to Learning Wherever You Are

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

- **Intensive courses** offered either in residence at Fort McNair or by distributed learning for students around the globe.
- **The 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, forums, workshops**, and other educational activities that faculty conduct to meet particular learning needs of organizations, and to address particular issues and topics.
- **Emerging Leader Workshops** to address the needs of future leaders and those who want to move to the next level of their careers. Geared toward GS-9s to GS-11s or equivalents, the workshop provides foundational education in the issues, challenges, and competencies of information leaders. The three-day Emerging Leader Workshop will be offered twice a year using an active learning model. Watch the IRM College website ([www.ndu.edu/irmc](http://www.ndu.edu/irmc)) for information about dates.





*“The programs and courses you offer will have significant relevance to my career. I see an immediate need for the application of the knowledge gained in my agency which can lead to increased responsibility and promotion.”*

*“Each time I take a course with the college I feel honored to be here. The professors are first rate and committed. I take a great deal of pride attending each and every course.”*

*“Instruction was just first rate. Outstanding, qualified faculty; they pushed us to think creatively and to apply what we learned.”*

The Senior Director of the IRM College provides strategic direction and vision for all faculty, staff, and students while the Dean of Faculty and Academic Programs oversees faculty, curriculum, and instruction. The Dean of Students and Administration oversees operational support for the College. The following three academic departments 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 certificates in IA: National Training Standard for Information Systems Security Professionals (NSTISSI No. 4011), National Information Assurance Training Standard for Senior Managers (CNSSI No. 4012), 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 Certificates.



## National Center of Academic Excellence in Information Assurance Education



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

## Joint Professional Military Education (JPME)

The IRM College provides instruction as a component of the Joint Professional Military Education (JPME) taught by the Industrial College of the Armed Forces (ICAF) and the National War College (NWC). The Information Operations Concentration Program, 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. Select electives may also be credited toward completion of the certificate programs offered by the College.



*Michael W. Carleton, Chief Information Officer, General Services Administration and NDU Hall of Famer, speaks at the April 2007 graduation in Marshall Hall.*





# PROGRAMS







The Advanced Management Program (AMP) is a 14-week resident graduate program designed for middle to senior managers who exercise leadership and carry responsibility for promoting and attaining national security, agency, and interagency goals through the use of information and/or information technology. The AMP is a highly interactive student-centered educational experience in which collaboration, communication, and critical thinking skills are modeled. The AMP prepares successful graduates to:

- **Lead within and across organizational boundaries** by leveraging information and information technology for strategic advantage;
- **Balance continuity and change** in the development, implementation, and evaluation of information resources management strategies and policies while meeting legislative and executive mandates;
- **Link critical decisions regarding people, processes, and technologies** to performance, results, and information assurance requirements;
- Commit to **ongoing leadership development** of self and others; and
- **Synthesize theory and best practices** from government, private sector, and not-for-profits to achieve the organization's mission.

The AMP has three elements that define its unique educational experience.

- First, the AMP curriculum's core and elective graduate-level courses provide a foundation in a broad range of information resources management disciplines. Graduates earn a Chief Information Officer (CIO) Certificate and can make progress toward completion of other certificates offered by the IRM College. Information Assurance Scholarship Program students are required to complete all four courses of the IA 4011 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, collaboration, leading change, and leading people. 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.
- Third, 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. 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:

- **Policy 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, 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.

- **Measuring Results of Organizational 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.
- **Strategies for Process Improvement:** 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, and 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.
- **Information Assurance and Critical Infrastructure Protection:** Provides a comprehensive overview of information assurance and critical information infrastructure protection, including information assets and protection of the information component of critical national infrastructures essential to national security. 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 knowledge management, capital planning, network security, and information operations. The curriculum map illustrates the various elements of the AMP.

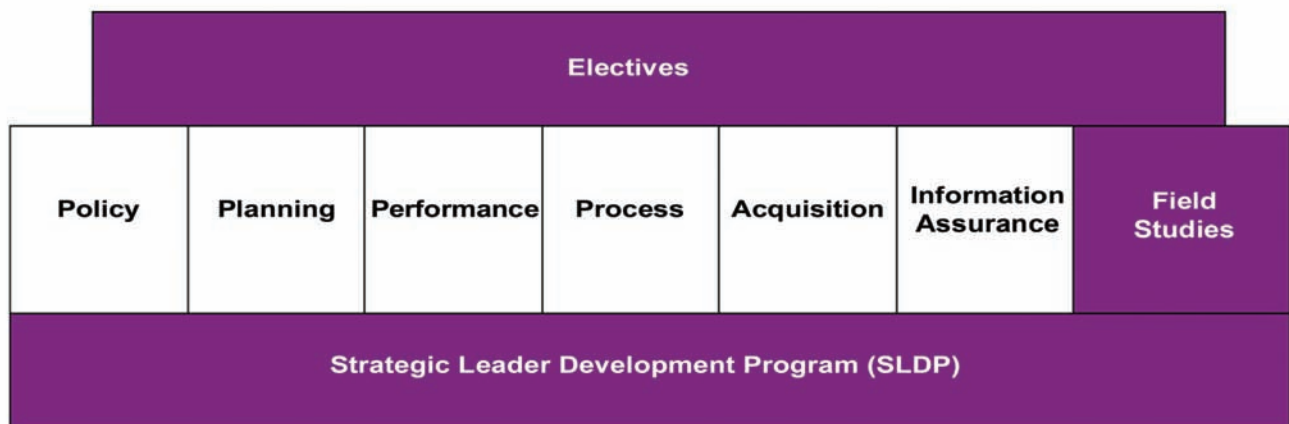


Figure 1.

## **AMP OFFERINGS**

### **Academic Year 2008**

AMP 35: September 10 – December 13, 2007

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

### **Academic Year 2009 (tentative dates)**

AMP 37: September 8 – December 12, 2008; applications due June 2, 2008

AMP 38: January 7 – April 17, 2009; applications due October 1, 2008

## **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 resume, a letter of nomination from the supervisor, and a completed AMP application form ([http://www.ndu.edu/irmc/AMP\\_Application\\_Form.pdf](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 may result in rejection of the application. Incomplete applications will be held by the IRM College for 60 days and then destroyed.

- **Resumé:** The resumé should include a work history that describes the candidate's position titles, organizations, responsibilities, and accomplishments, and any rewards or recognitions received. If there are gaps in the resumé, 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.
- **Waiver Requests:** Waiver requests may be included in the nomination packet. 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 (grade/rank or degree). 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](mailto:IRMCRegistrar@ndu.edu), or postal mail to:

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

**State and Local Government and Private Industry:** Applications for AMP must include a resumé, 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 defense agencies of other countries must apply through their governments. Applications should be in the form of an education and training request for approval and processing through the appropriate Security Assistance Training Field Activity (SATFA) country program manager, who should forward the request to:

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

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

The Advanced Management Program Director, Dr. Kathleen Schulin, can be contacted at [schulink@ndu.edu](mailto:schulink@ndu.edu).



*Linda Gooden, Executive Vice President, Information Systems & Global Services, Lockheed Martin Corporation addresses students during AMP.*



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 2.

The CIO Certificate Program is organized around 12 subject areas directly related to CIO competencies identified by the Federal CIO Council (see Figure 2). Subject areas across the multiple courses are offered to allow students to tailor their CIO program of study to meet their organization's needs and priorities (see Figure 3).

## 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:



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

*Richard "Dick" Burk, Chief Architect, Office of E-Government and Information Technology addresses an eResident class in Marshall Hall.*

<b>Required Core Courses (3 Courses)</b>		
<b>Key Competency Area</b>	<b>Course (Catalog Number)</b>	<b>Course Title</b>
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	AI (6203)	<i>Information Assurance and Critical Infrastructure Protection</i>
<b>Additional Core Courses (3 Courses from 3 different Key Competency Areas)</b>		
<b>Key Competency Area</b>	<b>Course (Catalog Number)</b>	<b>Course Title</b>
Acquisition	ITA (6415)	<i>Strategic Information Technology Acquisition</i>
Architectures and Infrastructures	ARC (6409)	<i>Enterprise Architectures for Managers</i>
	DMS (6414)	<i>Data Management Strategies and Technologies: A Managerial Perspective</i>
Capital Planning and Investment	BBC (6430)	<i>Building an IT Business Case</i>
	MTI (6315)	<i>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>
Project Management	ITP (6416)	<i>Information Technology Project Management</i>
Strategic Planning	IMP (6318)	<i>Information Management Planning</i>
	IWS (6202)	<i>Information Warfare and Military Strategy (Secret Clearance Required)</i>
Technology Assessment	CST (6510)	<i>Critical Information System Technologies</i>
<b>Other Courses (2 Courses)</b>		
Any course from the College Catalog		

Figure 3. CIO Certificate Program Requirements

# 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 4 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 EA Certificate requires successful completion of four core and three specialty courses (see Figure 3). The four core courses are *Information Management Planning (IMP)*, *Strategies for Process Improvement (PRI)*, *Enterprise Architecture for Managers (ARC)*, and *Data Management Strategies and Technologies (DMS)*. ARC must be successfully completed before enrolling in PMA, GIG, or FAC. 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* course (FAC). The final course in the EA Certificate is the *Enterprise Architecture Practicum (EAP)*. This course integrates knowledge and skills that students acquired in their prior courses through application in an organizational setting.

Core Courses			
Information Management Planning (IMP)	Strategies for Process Improvement (PRI)	Enterprise Architecture for Managers (ARC)	Data Management Strategies and Technologies (DMS)
Specialty Courses			
Global Information Grid (GIG)	OR	Federal Enterprise Architecture (FAC)	Planning and Managing Enterprise Architecture Programs (PMA)
Practicum Course			
Enterprise Architecture Practicum (EAP)			

Figure 4.



# INFORMATION ASSURANCE (IA) CERTIFICATES

The Information Assurance (IA) Program consists of several certificates that include 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 the national 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). 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 doctoral degree programs at several partner institutions of higher education.

## CERTIFICATE REQUIREMENTS

**NSTISSI No. 4011 Certificate Requirements:** This certificate requires completion of the following four courses:

- *Information Assurance and Critical Infrastructure Protection (AII)*
- *Global Enterprise Networking and Telecommunications (GEN)*
- *Cyber Security for Information Leaders (SEC)*
- *Enterprise Information Security and Risk Management (ESS)*



*IRM College faculty accept recertification as a National Center of Academic Excellence (CAE) in Information Assurance Education from the National Security Agency and the Department of Homeland Security.*

Students should begin the certificate by first taking the AII and GEN courses, 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 certificate.

**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)*.

**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.

- *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 Infrastructures and Key Assets (CIP)*



Figure 5.



The Information Technology Project Management (IT-PM) Certificate program is designed 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) Certificate.<sup>1</sup>

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 four core courses and two specialty courses. The core courses are *Strategic Information Technology Acquisition (ITA)*, *Critical Information Systems Technologies (CST)*, *Building an IT Business Case (BBC)*, and *Information Technology Project Management (ITP)*. Two specialty courses are required: *Software Acquisition Leadership (SAL)* and *Information Technology Program Leadership (IPL)*.

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

Figure 6.

<sup>1</sup>Project Management Professional (PMP) certification is offered by the Project Management Institute. Certification requires completion of a formal competency examination. Examination candidates must present evidence of having specified levels of general education and project experience and having successfully completed at least 35 contact hours of project management education. Details are available at the PMI website at <http://www.pmi.org>.



The explosive growth of technology innovations, economic globalization, and democratization of information has created a world of high complexity, interdependence, and uncertainty. Disruptive and unpredictable changes affect all aspects of organizations, often all at once. Successful and significant organizations embrace the opportunity to transform, by either responding to or shaping the new environment to accomplish mission goals, stretch their visions, and sustain strategic advantage.

The 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 OT 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 allows students 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.

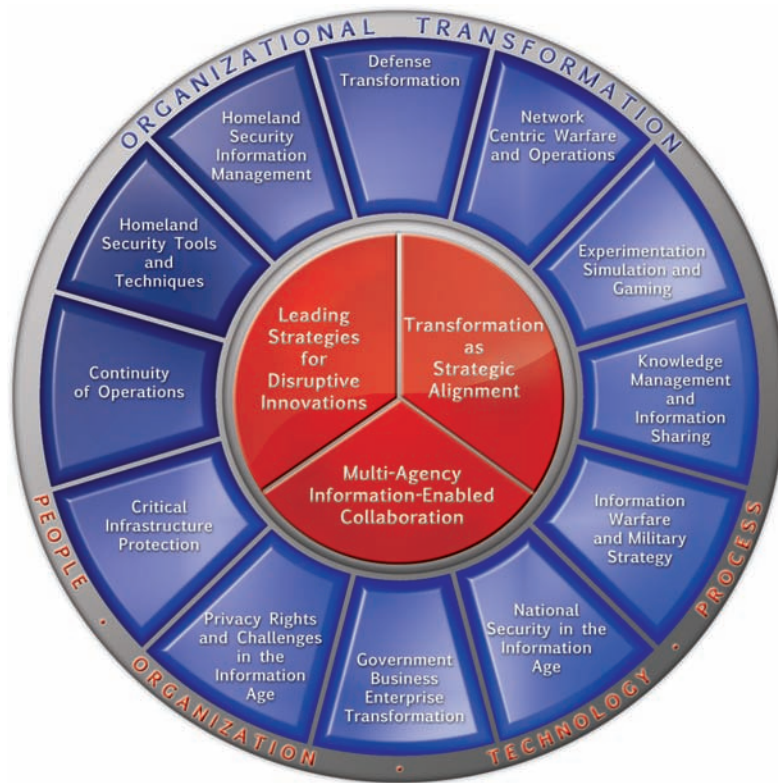


Figure 7.

## CERTIFICATE REQUIREMENTS

Award of the OT Certificate requires successful completion of eight courses. The three required courses are *Transformation as Strategic Alignment (TAS)*, *Multi-Agency Information-Enabled Collaboration (MAC)*, and *Leading Strategies for Disruptive Innovations (LSI)*. Students select five additional courses from the OT specialty courses. The specialty courses, building on the foundation courses, delve into particular aspects of defense and national security, homeland security, and national preparedness. 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.

<b>Required Core Courses (3 Courses)</b>	
<b>Course Title</b>	<b>Course (Catalog Number)</b>
Transformation as Strategic Alignment	TAS (6528)
Multi-Agency Information-Enabled Collaboration	MAC (6512)
Leading Strategies for Disruptive Innovations	LSI (6511)
<b>Required Specialty Course (Choose 5 Courses)</b>	
<b>Course Title</b>	<b>Course (Catalog Number)</b>
Defense Transformations	DTF (6509)
Network Centric Warfare and Operations	NCW (6513)
Experimentation, Simulation, and Gaming	ESG (6502)
Knowledge Management and Information Sharing	KMI (6506)
Information, Warfare, and Military Strategy	IWS (6202)
Information Operations and National Security in the Information Age	IOS (6207)
Government Business Enterprise Technology	GBE (6501)
Privacy Rights and Challenges in the Information Age	SPA (6508)
Protection of Critical Infrastructure and Key Assets	CIP (6212)
Continuity of Operations	COO (6504)
Homeland Security Tools and Techniques	HST (6503)
Homeland Security Information Management	HLS (6507)

Figure 8. OT Certificate Program Requirements



*IRM College offers all courses for either graduate/certificate credit (academic credit) or professional development.*

## **Professional Development**

The College welcomes students who want to enroll in individual courses to learn and to connect with others without seeking a certificate or academic credit by electing to take courses for professional development. In such cases, we will record a grade of Professional Development (PD) in the student's academic record and post it on the official NDU transcript. (Refer to the section on Grading for more information.) Students enrolled in certificate programs may take courses for PD; however, for courses to count toward a certificate or as a prerequisite, students must take them for credit.

Students taking courses for professional development will:

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

## **Professional Development Enrollment**

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

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

## **WHY YOU MIGHT CHOOSE A PROFESSIONAL DEVELOPMENT OPTION:**

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



## 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 University's uNET, an online student admission and enrollment management system. (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.

## 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.

**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 may be revoked and/or the student may be held liable for tuition owed.

### Requests to Waive Eligibility Requirements

**Exceptions:** The IRM College will consider requests for waivers for applicants who are within one grade level of the minimum eligible grade or who do not meet the minimum education requirement.

Students seeking either a grade or education requirement waiver should make their request via the "Employer Verification and Sponsorship Form," or the request should be on organizational or corporate letterhead and 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.

Students should submit supporting documents for admissions applications to the IRM College Registrar via fax (202-685-4860) or electronically as a scanned e-mail attachment sent to IRMRegistrar@ndu.edu.

Failure to submit required information or request for waiver consideration may result in denial of the request. The IRM College will hold incomplete applications for 60 days.

## APPLICATION INSTRUCTIONS

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.

Application Overview		
	Programs (non-AMP)	AMP
<b>ADMISSION</b>		
Application	Electronic, via uNET	Paper
Résumé required	No	Yes
Employer Verification and Sponsorship Form required	Yes, for NEW applicants or current/returning students with changes only	No
Nomination Letter required	No	Yes
Non U.S. Citizen Admission	via SAFTA country program manager	via SAFTA country program manager
<b>VERIFICATIONS</b>		
<i>Required upon Request</i>	Identity, education, employer, grade/rank	

### Application Processing Overview

When the Registrar's Office receives an online application, we will send the applicant a confirmation e-mail. The IRM College will review the application for eligibility and required documents. If a document is required (and not already in the office), we will send an e-mail to the applicant describing what needs to be provided. Once we receive all documents, we review the application send a notification to the applicant. (New students will also be sent a uNET Username and Password by e-mail, which can be used to self-register for courses.)

### Processing Time

The IRM College reviews all applications for completeness and applicant eligibility within 5 to 7 business days of receipt. The average admission processing time for a complete application is 10 to 15 business days. 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 e-mail IRMCRegistrar@ndu.edu.

## GENERAL APPLICATION INSTRUCTIONS

(Excluding AMP; see AMP section for detailed instructions)

### STEP ONE: Submit your application online.

The IRM College 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 forget or need the Username and Password, you must call the uNET help desk at 866-434-8883 (available 24 hours a day, 7 days a week).

### STEP TWO: Submit required documents.

**(verification forms and/or waiver letters)**

Students may submit letters and other application documents to the IRM College Registrar via fax (202-685-4860) or as a scanned e-mail attachment sent to IRMCRegistrar@ndu.edu. We will hold incomplete applications for 60 days and then destroyed.

### 1. NEW Applicants: Employer Verification and Sponsorship Form

A. Government Employees:

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 IRMCRegistrar@ndu.edu).

B. Private Sector (Industry/Contractor) Applicants Only:

The applicant's **sponsoring government agency's contract coordinator** (or his/her most immediate supervisor) 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 IRMCRegistrar@ndu.edu).

The applicant may attach additional comments. A downloadable version of the form template is available on the IRM College website ([www.ndu.edu/irmc](http://www.ndu.edu/irmc)).

## Employer Verification and Sponsorship Form Template

### \*Applicant Information:

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

### \*Employer Representative (Supervisor, HR Officer, or Sponsor) Information:

5. Name:
6. Organization Name:
7. Your 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 answer No/uncertain to either #13 or #14, 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):

### \*Contract Information: PRIVATE SECTOR (Industry/Contractor) APPLICANTS ONLY

16. The applicant is performing work directly supporting the scope of a valid government agency contract: \_\_\_ Yes \_\_\_ No
17. The number of the contract being supported:

### \*Certification:

18. Employer Representative Signature:
19. Date (mm/dd/yy):

## 2. Waiver Letter:

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

## STEP THREE: Receive program acceptance notification.

All applications are reviewed for completeness and applicant eligibility within 5 to 7 business days of receipt. Questions concerning status of pending applications should be addressed to the Registrar's Office by phone (202-685-6300; DSN 325-6300) or e-mail to IRMCRegistrar@ndu.edu.

### Communications of IRM College Admission

**Decisions:** Applicants to programs will receive both an e-mail notification and a formal letter to notify them of the IRM College Admissions 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.

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.

**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.

FY08: The FY 2008 intensive course fee for non-DoD federal, state, and local government employees is \$1,100. The FY 2008 intensive course fee for private industry students is \$1,995.

FY08: 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

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

Students enrolled in AMP should make their payments prior to the first day of the AMP. If we do not receive an AMP student's payment, the student will need to reapply for a future offering.

IRM College cannot accept cash payments. Valid forms of payment are credit card, U.S. Treasury check, electronic funds transfer, and Military Interdepartmental Purchase Request (MIPR).

Detailed instructions for submitting payment are 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

The IRM College will assign the student an account, Username, and Password that he/she will use to self-enroll in classes from uNET (link from [www.ndu.edu/irmc](http://www.ndu.edu/irmc)) once accepted into an academic program. If a student experiences any problems accessing accounts or enrolling in classes, he/she may contact the Registrar's Office by phone (202-685-6300; DSN 325-6300) or e-mail at [IRMCRegistrar@ndu.edu](mailto:IRMCRegistrar@ndu.edu).

### Enrolling With the Class Number

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

1. Log into uNET (using your Username and Password)
2. Click on "Add/Drop a Class"
3. Select "Academic Year 200X/200X"
4. Select "Add Classes"
5. Enter Class Number

6. Click "Submit"
7. 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. Click on "Add/Drop a Class"
3. Select "Academic Year 200X/200X"
4. Click on the magnifying glass next to the Class Number box
5. In the Subject box, enter "IRMC-INT"
6. In the Description box, enter the three-letter course description (e.g., ARC, GEN, SEC, etc.)
7. *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.
8. Click on "Search"
9. Click on the checkbox next to the class you want to attend
10. Click "Submit"
11. Click "View My Schedule"

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

### Confirmation of Enrollment

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

### Enrollment Limits

Students may not enroll in more than one eResident or two distributed learning courses in the same time frame (start-date to end-date).

### Pre-course Materials and Assignments

Each course has Blackboard-accessible readings and other pre-course activities that allow students to prepare for the first day of their course. Pre-course materials will be posted

to the IRM College's eLearning system (Blackboard) no earlier than 13 days before the start of class.

### **No Show Policy**

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

### **Dropping a Course in uNET**

If your schedule prevents your participation in a scheduled course, we request you drop the course prior to the start date in uNET. [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. Click on "Add/Drop a Class"
3. Select "Academic Year 200X/200X"
4. Select "Drop/Update Classes"
5. You will now see all classes you are enrolled in
6. Select "Drop" in the Action field next to the class or classes that you are dropping
7. Click "Submit"
8. Click "View My Schedule"

## **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 annually 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.** 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 (e.g., lost in a fire) may contact the Registrar's Office via e-mail at [IRMCRegistrar@ndu.edu](mailto:IRMCRegistrar@ndu.edu) for further guidance.

### **Graduation Exercises**

The IRM College Graduation Exercise for Academic Year 2008 is tentatively scheduled for April 10, 2008 (check the IRM College website for exact date and time). The Registrar will contact all known and potential graduates at the students' preferred e-mail address as shown in uNET approximately eight weeks prior to graduation. This e-mail message will provide detailed timelines and procedures that students must follow to be included in graduation planning.

Students who are attempting to complete their programs within two months of graduation are advised to work closely with their faculty advisor and course instructors to ensure they meet requirements in time for graduation.

### **Transcripts**

Two types of transcripts are available from the IRM College.

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

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

## ACADEMIC 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 four years.

### Applying Coursework Earned Prior to Program Admission

If a participant has completed IRM College coursework under another program, he/she may apply eligible courses to another 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 four years.

If you need to request an exception to the application of previous IRM College academic work to a new program, you may e-mail your request with a justification to [IRMCEXceptionRequest@ndu.edu](mailto:IRMCEXceptionRequest@ndu.edu). We will e-mail a response 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.** The IRM College will drop students from a 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 [IRMCEXceptionRequest@ndu.edu](mailto:IRMCEXceptionRequest@ndu.edu). Confirmation of withdrawal will be provided by e-mail.

**Reinstatement.** The IRM College may grant reinstatement to a certificate program on a case-by-case basis. Students who wish to request reinstatement must e-mail their requests, along with justification or explanation of extenuating circumstances, to [IRMCEXceptionRequest@ndu.edu](mailto:IRMCEXceptionRequest@ndu.edu). We will send a response by e-mail to the address originating the request.

## GRADING

The IRM College's grading system follows:

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



- **No Credit (NC):** When an “NC” grade is assigned, the student will not receive academic credit for the class. This grade is used when:
  - o Attendance/participation requirements are not met.
  - o 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).
  - o Students enrolled in Distributed Learning (DL) courses do not participate by the end of the third week and are dropped by the faculty.
  - o Students withdraw after 25 percent of the course has been taught (e-resident or DL).
  - o Students do not meet academic requirements on resubmission of an unacceptable academic requirement.
  
- **Incomplete (I):** This grade is assigned to a student who:
  - o 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.
  - o 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](mailto:IRMCEXceptionRequest@ndu.edu).

- **Withdraw (W):** When the student requests withdrawal from a course after the start date but within the first 25 percent of the course, the faculty member will assign a grade of “W”. The request to withdraw must be submitted in writing to the Offering Leader. If the student requests withdrawal after 25 percent of the course is completed, the faculty member will assign a grade of “No Credit.”
  
- **Professional Development (PD):** This grade is assigned to students who elect to take a course for professional development and successfully complete requirements. Students do not receive academic credit for

professional development courses. Students must retake courses for credit if they want to apply them to a certificate program.

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

#### **Other Annotations:**

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

## **ACADEMIC INTEGRITY**

The College 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.

Plagiarism is the unauthorized use, intentional or unintentional, of intellectual work of another person without providing proper credit to the author. While most commonly associated with writing, all types of scholarly work, including computer code, speeches, slides, music, scientific data and analysis, and electronic publications are not to be plagiarized. Students are encouraged to submit their papers and assessments through SafeAssignment found in the Student Success Course in Blackboard prior to turning them in for grading.

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 authority for decisions and actions rests at 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**

The end-of-course survey provides students the opportunity to provide feedback on the instruction, materials, and intended learning outcomes. 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 students should submit their comments on various aspects of course design and delivery. Survey results are shared with the faculty and the college leadership and are used as a basis for future course revisions. The end-of-course survey results are aggregated and not attributable to any individual.

## **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.

## **INSTRUCTIONAL FORMATS**

Intensive program courses are available in two formats:

- The e-Resident format uses a blended approach to engage learners in various learning activities:
  - o Pre-course materials in Blackboard (Bb): Students may access course materials up to 13 days prior to the start date of the course through our online learning platform, Blackboard.
  - o In-residence portion: Students attend a one-week in-residence portion (see published Schedule of Classes for dates).
  - o 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.
  - o 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.)

# 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
DMS	Data Management Strategies and Technologies: A Managerial Perspective	6414
DTF	Defense Transformation	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
GBE	Government Business Enterprise Transformation	6501
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	Cyber Security for Information Leaders	6201
SPA	Privacy Rights and Challenges in the Information Age	6508
TAS	Transformation as Strategic Alignment	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, students are strongly recommended to take this course as the first in the NSTISSI No. 4011 certificate.

### **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

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

### 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.

### 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**

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

### **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.

### **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.

### **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, students are recommended to take this course as the first 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.

# 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 TRANSFORMATION

Subject: IRMC-INT  
Catalog Number: 6509

### COURSE DESCRIPTION

This course focuses on transformation initiatives relating to DoD capabilities, forces, and the Defense business 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 recent and current Revolutions in Military and Business Affairs. This is followed by a prospective context examining the innovations in formation 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 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 as they seek to transform a complex mega-enterprise while simultaneously preparing and leading global war-fighting and peace building operations.

### RECOMMENDED ATTENDANCE

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

### LEARNING OUTCOMES

Students will be able to formulate and shape the requirement for future transformation initiatives; develop strategies that prepare defense organizations to successfully engage in and achieve transformational change; appraise critically the ends, ways and means of defense transformation; and from these assessments develop strategies for transformation, and their supporting execution and transition roadmaps that can be successfully proposed and endorsed.

# 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 e-Government and e-Governance 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 e-Government and boundary-spanning programs and IT initiatives. Governance models, legislation, policies, and current e-Government 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 e-Government, 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 e-Government models, initiatives, and approaches, the course provides a policy foundation for assessing the issues attendant to transforming government and governance.

### **LEARNING OUTCOMES**

Students will be able to explain the ideas, policies, and programs of e-Government initiatives; assess the ongoing transformation in governance and its processes; and articulate the leadership and managerial challenges posed by e-Government 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.

### **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; however, students should take this course as the last course in the NSTISSI No. 4011 Certificate.

### **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 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.

# GBE

## **GOVERNMENT BUSINESS ENTERPRISE TRANSFORMATION**

Subject: IRMC-INT

Catalog Number: 6501

### **COURSE DESCRIPTION**

This course focuses on initiatives, strategies, and opportunities for transforming the federal government's business operations that provide capabilities, resources, and materiel to the government employee (such as global war-fighters or disaster recovery staff). 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 Federal Enterprise Architecture as the information technology enabler of business enterprise transformation are evaluated. Students examine large organization transformations from the corporate sector to identify insightful lessons that can be developed as recommendations for government business enterprise transformation.

### **RECOMMENDED ATTENDANCE**

The course is critical for DoD officers and Federal civilian executives who hold or aspire to hold leadership positions with transformation responsibilities.

### **LEARNING OUTCOMES**

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

# GEN

## **GLOBAL ENTERPRISE NETWORKING AND TELECOMMUNICATIONS**

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 non-technical 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, students should take this course as the second in 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 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 interrelationship 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.

### **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)* course 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 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.

### **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 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.

### **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.

### **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.

### **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, students should successfully complete *Strategic Information Technology Acquisition (ITA)* before taking this course.

### **LEARNING OUTCOMES**

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

# 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 at the theater and strategic levels. The course emphasizes interagency and international considerations in the planning and conduct of Information Operations (IO). The course also examines selected non-U.S. approaches to the strategies for and uses of the full spectrum of information operations by current and potential global competitors and adversaries. A lesson on strategic legal implications and considerations is also presented, and an in-class exercise examines the use/misuse of IO strategies against an adaptive adversary. The course concludes with a snapshot of current U.S. military IO strategies.

### **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.

### **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. ge organizations.

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

### **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 transformational responsibilities.

### **LEARNING OUTCOMES**

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

# MAC

## **MULTI-AGENCY INFORMATION-ENABLED COLLABORATION**

Subject: IRMC-INT  
Catalog Number: 6512

This course focuses on strategies, means, and information models needed to pursue multi-agency collaboration to support 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 includes multilateral collaboration situations with nongovernment (NGO) and international organizations, media, and coalition partners. The relevance and adaptations to current and future multi-agency and multilateral collaboration situations are also assessed. The course examines how information-enabled networks, collaborative tool-sets, cross-boundary information-sharing and work processes, professional development experiences, and alternative coordination architectures can be harnessed in support of effective multi-agency and multilateral national and homeland security activities. Impediments such as legal and budgetary authority restrictions, educational, and cultural factors that inhibit cross-boundary mission effectiveness and transformation are assessed, as are strategies for addressing them.

### **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.

### **LEARNING OUTCOMES**

Students will be able to formulate and shape transformation initiatives aimed at expanding missions that require multi-agency collaboration, coordination, and cooperation; appraise critically the ends, ways, and means, including tools, technologies, and work practices, of highly effective multi-agency collaboration, coordination, and cooperation; and develop, propose, and defend recommendations for transformation strategies aimed at effective multi-agency collaboration and their supporting execution and transition plans.

# 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**

This course should be 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.

### **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.

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

### **RECOMMENDED ATTENDANCE**

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

### **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. They will be able to provide advice on the implementation challenges of process improvement, including impacts upon organizational culture, structure and governance, and design and propose initiatives and actions for addressing such challenges.

# 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.

### **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, students are encouraged to have successfully completed *Strategies for Process Improvement (PRI)*.

### **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**

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

### **LEARNING OUTCOMES**

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

# SEC

## **CYBER SECURITY FOR INFORMATION LEADERS**

Subject: IRMC-INT  
Catalog Number: 6201

### **COURSE DESCRIPTION**

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

### **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, students should complete *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 cyber-security posture of an organization to determine adequate people, processes, 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.

### **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.



# TAS

## 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 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.

### 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.



“Attending classes at the College has been the highlight of my work life for the past two years. I have enjoyed each and every class I have attended. Thank you!”

“Thank you for the contributions you have made to my career, my learning, and my life. I am greatly indebted for the time and knowledge you have shared along the way.”

“The IRM College is an excellent educational institution with a real mission of providing highly qualified senior leaders for the federal government capable and motivated to be good stewards for the American taxpayer. Thank you for the outstanding education you provide.”

# ACADEMIC PARTNERSHIP PROGRAM



The IRM College forms 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 to complete a master’s or doctoral degree. Partner institutions will accept between 9 and 15 graduate credits depending on which certificate program a student completed at the IRM College. Our academic partners provide full-time, part-time, and online educational opportunities.

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 for specific details relating to the number of courses remaining to satisfy degree requirements and admission criteria for IRM College graduates.

The IRM College actively seeks to develop new academic partnerships based on strategic requirements. Discussions with several potential partners are currently underway, and those universities do not appear on the list. Please check the IRM College website for the most current version of this listing ([http://www.ndu.edu/irmc/ntwk\\_list1.htm](http://www.ndu.edu/irmc/ntwk_list1.htm)). Contact the Partnership Coordinator, Patty Coopersmith at ([coopersmithp@ndu.edu](mailto:coopersmithp@ndu.edu), 202-685-2117), for more information.



*Dr. Robert Childs and Patty Coopersmith showcase the Best Practice Award awarded to the College for its Academic Partner Program from the Corporate University Xchange.*

<b>IRM College Academic Partners</b>	
<b>University</b>	<b>Degrees Available per Partnership Agreement</b>
<b>Auburn University (AL)</b> Samuel Ginn College of Engineering  John “Drew” Hamilton <a href="mailto:hamilton@eng.auburn.edu">hamilton@eng.auburn.edu</a> 334-844-6360	<u>Master of Software Engineering</u> (Additional 24 credits required; some online courses available.) (IASP qualified.)  9 credit hours for IRM College IA 4011 Certificate graduates.

<p><b>Capitol College (MD)</b> Graduate School</p> <p>Ken Crockett ken@capitol-college.edu 301-369-2800, ext. 3025</p>	<p><u>Master of Science in Information and Telecommunications Systems Management (ITSM);</u> <u>Master of Science in Information Assurance (MSIA);</u> <u>Master of Business Administration (MBA)</u> Additional 22–31 credit hours required depending on degree chosen and IRM College certificate completed; traditional and/or online classes; full-or part-time, credit hours applied to specific courses.</p> <p>9 credits accepted for IA 4011 Certificate graduates; 12 for students who complete both the IA 4011 and IA 4012 Certificates; 12 for graduates of the IT Project Management Certificate; 12 for graduates of the Enterprise Architecture Certificate; or 15 credit hours accepted for CIO, CISO, and AMP Certificate graduates.</p>
<p><b>Clemson University (SC)</b> Technology and Human and Organizational Development Department</p> <p>Philip McGee pmcgee@clemson.edu 864-250-6719</p>	<p><u>Masters in Human Resource Development</u> (additional 21 semester hours required).</p> <p>15 credit hours accepted for Organizational Transformation Certificate graduates.</p>
<p><b>Central Michigan University (MI)</b> College of Graduate Studies</p> <p>Mary Pat Mabeus Marypat.mabeus@cmich.edu Fort Belvoir, VA campus 703-360-5336</p> <p>D. Ernest Bedford bedfo1de@cmich.edu Mount Pleasant, MI campus 989-774-4464</p>	<p><u>Master of Science in Administration (concentrations in Information Resource Management, Leadership, or General Administration)</u> (Additional 21–24 hours required).</p> <p>12 graduate credit hours accepted for graduates of the Enterprise Architecture Certificate or the IT-Project Management Certificate; or 15 credits for the Chief Information Officer Certificate or the Organizational Transformation Certificate.</p>
<p><b>East Carolina University (NC)</b> School of Industry and Technology</p> <p>Biwu Yang yangb@mail.ecu.edu 252-328-9666</p>	<p><u>MS in Industrial Technology (MSIT), concentration in Digital Communication, Computer Networking Management, or Information Security</u> (Additional 21–27 credit hours required; credit hours applied to specific courses; courses available online.)</p> <p>15 credit hours accepted for AMP graduates or CIO Certificate graduates; or 9 credit hours for IA 4011 Certificate graduates.</p>
<p><b>Eastern Michigan University (MI)</b> College of Technology, School of Technology Studies</p> <p>Gerald “Skip” Lawver Skip.lawver@emich.edu 734-487-1590</p>	<p><u>Master of Liberal Studies (concentration in Information Assurance)</u> (Additional 15–21 credit hours required depending on IRM College certificate completed.)</p> <p>15 credits for CIO Certificate graduates, or 9 credit hours for IA 4011 Certificate graduates.</p>

<p><b>George Mason University (VA)</b> 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> (Additional 21 credit hours required after IRMC certificate completion.)</p> <p>15 credit hours accepted for AMP graduates or CIO Certificate graduates.</p>
<p>School of Information Technology &amp; Engineering</p> <p>Daniel Menasce menasce@gmu.edu 703-993-1505</p> <p>Sushil Jajodia jajodia@gmu.edu 703-993-1653</p> <p>Jeremy E. Allnutt jallnutt@gmu.edu 703-993-3810</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 (MS-SWE);</u> (All master's degrees require additional 21 credit hours.)</p> <p><u>PhD in Information Technology; PhD in Computer Science</u> (Number of credit hours for PhD depends on master's degree transferred; credit hours applied towards specific courses.)</p> <p>9 credit hours accepted for IA 4011 Certificate graduates.</p> <p><u>Master of Science in Telecommunications</u> (Additional 21 credit hours; credits applied towards specific courses.)</p> <p>9 credit hours accepted for IA 4011 Certificate graduates.</p>
<p><b>Georgia Institute of Technology (GA)</b> Sam Nunn School of International Affairs &amp; Ivan Allen College of Liberal Arts</p> <p>Seymour "Sy" Goodman Goodman@cc.gatech.edu 404-385-2271</p>	<p><u>MS in International Affairs</u> (Additional 25 credits required.)</p> <p>9 credit hours accepted for IA 4011 Certificate graduates.</p>
<p><b>James Madison University (VA)</b> College of Graduate and Professional Programs</p> <p>Kenneth Bahn bahnkd@jmu.edu 540-568-3009</p> <p>Department of Computer Science</p> <p>Hossain Heydari heydarmh@jmu.edu 540-568-8745</p>	<p><u>Master of Business Administration, concentration in Information Security</u> (Additional 30-36 credit hours required; credits applied towards specific courses; primarily online.)</p> <p>15 credit hours accepted for AMP graduates or CIO Certificate graduates who also completed the IA 4011 Certificate; or 9 credit hours accepted for IA 4011 Certificate graduates.</p> <p><u>Master of Science in Computer Science (concentration in Information Security)</u> (Additional 24 credit hours required; credits applied towards specific courses; cohort online learning.)</p> <p>9 credit hours accepted for IA 4011 Certificate graduates.</p>
<p><b>Johns Hopkins University (MD)</b> 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> (Additional 21 credit hours required; credits applied to specific courses.)</p> <p>9 credit hours accepted for IA 4011 Certificate graduates.</p>

<p><b>Mississippi State University (Master of Science)</b> Bagley College Of Engineering</p>	<p><u>MS in Computer Science (MSC)</u> (Additional 20 credit hours required; some courses available online, some residency requirements.) <u>PhD in Computer Science</u> (Additional 28 hours of coursework and 20 hours dissertation research required; some residency requirements.)</p> <p>15 credit hours for AMP graduates or CIO Certificate graduates who also complete the IA 4011 Certificate; or 9 credit hours for IA 4011 Certificate graduates.</p>
<p>College of Business and Industry</p> <p>Dave Dampier dampier@CSE.MsState.edu 662-325-8923</p>	<p><u>MS in Information Systems (MSIS)</u> (Additional 15 credit hours required; credit applied to specific courses); <u>MBA in Project Management</u> (Additional 23 hours required); <u>PhD in Business Administration</u> (major in Information Systems) (Additional 39 hours required.)</p> <p>15 graduate credit hours accepted for AMP graduates or CIO Certificate graduates.</p>
<p><b>New Mexico Tech (NM)</b> Department of Computer Science</p> <p>Dr. Andrew H. Sung sung@cs.nmt.edu 505-835-5126</p>	<p><u>PhD in Computer Science</u> (Additional 36–42 hours required depending on which IRM College certificate completed.)</p> <p>9 credit hours accepted for IA 4011 Certificate graduates, or 15 credit hours accepted for CIO Certificate graduates.</p>
<p><b>Northeastern University (MA)</b> 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 IA4011 Certificate graduates.</p>
<p>School of Professional and Continuing Studies</p> <p>Leslie Schneider l.schneider@neu.edu 617-373-4766</p>	<p><u>Master of Professional Studies in Informatics</u> (Additional 20–28 quarter hours required depending on IRM College certificate completed; online options.)</p> <p>9 credit hours accepted for IA 4011 Certificate graduates; or 15 credit hours for CIO Certificate graduates. (MPSI degree)</p> <p><u>Master of Science in Leadership</u> (Additional 21 quarter hours required.) 15 credit hours accepted for Organizational Transformation (OT) Certificate graduates. (MSL degree)</p>
<p><b>Pace University (NY)</b> School of Computer Science and Information Systems</p> <p>Bernice Houle bhoule@pace.edu 914-773-3592</p>	<p><u>MS in Internet Technology; MS in Computer Science; MS in Information Systems</u> (Additional 21–27 credit hours required depending on IRM College certificate completed.)</p> <p>15 credit hours for CIO Certificate graduates; or 9 credit hours for IA 4011 Certificate graduates.</p>

<p><b>Polytechnic University (NY)</b> Computer Science Department</p> <p>Nasir Memon memon@poly.edu 718-260-3970</p>	<p><u>MS in Computer Science</u> (Additional 27 credits required.)</p> <p>9 credit hours accepted for IA 4011 Certificate graduates.</p>
<p><b>Regis University (CO)</b> School of Professional Studies</p> <p>Donald Archer archer@regis.edu 303-458-4335</p>	<p><u>MS 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><b>San Diego State University (CA)</b> College of Business Administration</p> <p>Bruce Reinig breinig@mail.sdsu.edu 619-594-3032</p>	<p><u>MSBA in Information Systems</u> (Additional 18 credits required, possible prerequisites).</p> <p>12 credit hours accepted for Enterprise Architecture (EA) Certificate graduates or for IT Project Management (IT-PM) Certificate graduates.</p>
<p><b>Syracuse University (DC, NY)</b> School of Information Studies</p> <p>Kathy Allen kallen02@syr.edu 315-443-4251</p>	<p><u>MS in Information Resource Management</u> (concentration in Information Assurance or Enterprise Architecture) (Additional 15–21 credit hours required depending on IRM College certificate completed; courses available at the Washington, D.C. campus, online, or at the Syracuse, NY campus.)</p> <p>15 credit hours accepted for AMP graduates or CIO Certificate graduates; or 12 credit hours for Enterprise Architecture (EA) graduates; or 9 credit hours for IA 4011 Certificate graduates.</p>
<p><b>Texas A&amp;M University (TX)</b> Center for Information Assurance and Security</p> <p>Wei Zhao w-zhao@tamu.edu 979-845-9776</p>	<p><u>MS in Computer Science; MS in Computer Engineering; Master of Computer Science; Master of Engineering in Computer Engineering; MS in Electrical Engineering; Master of Engineering in Electrical Engineering; MS in Management and Information Systems; Ph.D. in Computer Science; Ph.D. in Computer Engineering; PhD in Electrical Engineering; PhD in Information and Operations Management.</u> (Additional 21–24 credits for Master’s; 52 hours for PhD if Master’s was in an approved program, 84 if Master’s was not in a related field.)</p> <p>9 credits accepted for IA 4011 Certificate graduates (possibly more credits for those students who complete both the CIO Certificate and the IA 4011).</p>
<p><b>Towson University (MD)</b> Center for Applied Information Technology</p> <p>Lisa Loewe mloewe@towson.edu 410-704-4909</p>	<p><u>Master of Science in Applied Information Technology</u> (Additional 18–24 hours required depending on IRMC certificate completed; credits applied to specific courses.)</p> <p>15 credit hours accepted for AMP graduates or CIO Certificate graduates who also completed the IA4011 Certificate; or 12 credit hours for students with both IA4011 and IA4012 Certificates; or 9 credit hours for IA4011 Certificate graduates.</p>

<p><b>University of Dallas (TX)</b> Graduate School of Management</p> <p>Blake Frank bfrank@gsm.udallas.edu 972-721-4091</p>	<p><u>Master of Business Administration, concentration in Information Assurance (MBA/IS)</u> (Additional 34-40 hours required.) <u>Master of Management in Information Assurance</u> (Additional 16–22 hours.) <u>Master of Science in Information Assurance</u> (Additional 16–22 hours.) (All courses available online and remaining hours depend on IRM College certificate completed.)</p> <p>15 credit hours accepted for AMP graduates or CIO Certificate graduates; or 9 credit hours for IA 4011 Certificate graduates.</p>
<p><b>University of Detroit Mercy (MI)</b> College of Business Administration</p> <p>Dan Shoemaker dshoemaker1@twmi.rr.com 313-993-1170</p>	<p><u>Master of Science in IA; Master of Science in Computer and Information Systems.</u> (Additional 15–21 credits required depending on IRM College certificate completed.)</p> <p>9 credits for IA 4011 Certificate graduates; or 12 credits for students with both IA 4011 and IA 4012 Certificates; or 15 credits for CIO Certificate graduates who also completed the IA 4011; or 15 credits for Chief Information Security Officer (CISO) Certificate graduates.</p>
<p><b>University of Illinois at Urbana-Champaign (IL)</b> Department of Computer Science</p> <p>Roy H. Campbell rhc@cs.uiuc.edu</p>	<p><u>Master of Computer Science; Master of Science in Computer Science; Master of Science in Bioinformatics</u> (Additional 27 credits required.)</p> <p>9 credit hours accepted for IA 4011 Certificate graduates.</p>
<p><b>University of Maryland, Baltimore County (MD)</b> 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; Master of Science in Computer Engineering</u> (Additional 24 credit hours, prerequisites and GRE required; resident only.)</p> <p>9 credit hours accepted for IA 4011 Certificate graduates.</p>
<p><b>University of Maryland University College (MD)</b> Graduate School of Management &amp; Technology</p> <p>Paul Keller pkeller@umuc.edu 301-985-4616</p> <p>Jim Cronin jcronin@umuc.edu 240-684-5153</p> <p>Robert Ouellette rouellette@umuc.edu 301-985-7833</p>	<p><u>MS in Computer Systems Management (CSMN); MS in Telecommunications Management (TLMN); MS in Information Technology (MSIT).</u> (Additional 21-24 credit hours required; courses available online; credit hours applied to specific courses.)</p> <p>15 credit hours accepted for AMP graduates or CIO Certificate graduates.</p> <p><u>Doctor of Management</u> (48–60 hours required), online available. 12 credits accepted for graduates with both IA 4011 and IA 4012 Certificates; 12 credits for Organizational Transformation Certificate graduates; or 9 credits for IA 4011 graduates.</p> <p><u>MS in Electronic Commerce</u> (Additional 21 credits required; credits applied to specific courses.)</p> <p>15 credit hours for Organizational Transformation (OT) or e-Government Certificate graduates.</p>

<p><b>University of Nebraska at Omaha (NE)</b> 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> (Additional 21 credits required after IRM College certificate).</p> <p>15 credit hours for AMP graduates or CIO Certificate graduates (who also earned IA 4011 certification). (Note: Specific IRM College courses are required for the credit acceptance – CWC, LDC, and DMS.)</p>
<p><b>University of North Carolina at Charlotte (NC)</b></p> <p>Bill Chu billchu@uncc.edu 704-687-4568</p>	<p><u>Master of Science in Information Technology (MSIT)</u> (Additional 15–21 credit hours required; residence only.)</p> <p>15 credit hours for AMP graduates or CIO Certificate graduates (who also earned IA 4011 Certification); or 9 credit hours for IA 4011 Certificate graduates.</p>
<p><b>University of Pittsburgh (PA)</b> Department of Information Sciences and Telecommunications</p> <p>James Joshi jjoshi@mail.sis.pitt.edu 412-624-9982</p>	<p><u>MS in Information Science (MSIS);</u> <u>MS in Telecommunications and Networking (MST&amp;N)</u> (Additional 21 to 27 credits required.)</p> <p>15 credit hours for AMP graduates or CIO Certificate graduates (who also earned IA 4011 concentration); or 9 credit hours for IA 4011 Certificate graduates.</p>
<p><b>University of Texas at San Antonio (TX)</b> College of Business</p> <p>Glen Dietrich gdietrich@utsa.edu 210-458-5354</p>	<p><u>Master of Science in Information Technology (IA concentration)</u> (Additional 18–24 credit hours required.)</p> <p>15 credit hours for AMP graduates or CIO Certificate graduates (who also earned IA 4011 certification); (Note: The following IRM College courses are required for the 15 credits to be accepted: LDC, PRI); or 9 credit hours for IA 4011 Certificate graduates.</p>
<p><b>University of Tulsa (OK)</b> 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> (Additional 15–21 credit hours required; credits applied to specific courses; residence only.)</p> <p><u>Doctor of Philosophy in Computer Science (concentration in Information Assurance)</u> (Additional 75–81 credit hours required, 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.)</p> <p>15 credit hours for AMP graduates or CIO Certificate graduates; or 9 credits for IA 4011 Certificate graduates.</p>



<p><b>Walsh College (MI)</b> Information Assurance Center</p> <p>Nanette Poulis npoulis@walshcollege.edu 248-689-8282</p>	<p><u>Master of Science in Information Assurance</u> (Additional 21–36 hours required depending on IRMC certificate completed and other prior coursework.)</p> <p>15 credit hours for Chief Information Security Officer (CISO) Certificate graduates; or 12 credit hours for students who complete both the IA4011 and IA4012 Certificates, or 12 credit hours for IT Project Management (IT-PM) Certificate graduates; or 9 graduate credit hours accepted for IA4011 Certificate graduates.</p>
<p><b>University of Washington (WA)</b> Department of Urban Design and Planning</p> <p>Hilda Blanco hblanco@u.washington.edu 206-616-9057</p>	<p><u>Masters in Strategic Planning for Critical Infrastructures</u> (additional 40 quarter credits (30 semester credits) required) (IASP qualified).</p> <p>9 semester (12 quarter) credit hours accepted for students who complete the Information Assurance (IA) 4011 Certificate. Offered fully on-line.</p>

The table is current as of the catalog print date. Please check IRM College website ([http://www.ndu.edu/irmc/ntwk\\_list1.htm](http://www.ndu.edu/irmc/ntwk_list1.htm)) for updates on degrees and new partner universities.

## 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; Ph.D., The University of Phoenix.



*Dr. Stan Boddie accepts the Professor of the Year Award at the 2007 IRM College graduation ceremony.*

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.

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. CLAVADTSCHER, 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; B.A., Western Illinois University; M.B.A., St. Ambrose University; D.B.A., Nova Southeastern 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, 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; B.Sc., Nottingham University (United Kingdom); M.Sc., 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.

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

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., Ph.D., The George Washington University.

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

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., Industrial College of the Armed Forces; M.S., Troy State University; 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.

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



# 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 5<sup>TH</sup> AVE, BLDG 62  
FORT MCNAIR, DC 20319  
202.685.6300

[WWW.NDU.EDU/IRMC](http://WWW.NDU.EDU/IRMC)



NATIONAL DEFENSE UNIVERSITY