



**College of Information and Cyberspace  
Schedule of Courses  
Academic Year 2026-2027  
Fall Trimester**





## CONTACT DIRECTORY

### **INTERNET HOME PAGE:**

<http://cic.ndu.edu/>

### **TELEPHONE:**

202-685-6300

DSN 325-6300

### **E-MAIL:**

[CICOSS@ndu.edu](mailto:CICOSS@ndu.edu)

### **MAILING ADDRESS:**

College Of Information and Cyberspace

Office of Student Services

300 5<sup>th</sup> Avenue, Bldg 62, Rm 145

Ft. Lesley J. McNair, DC 20319-5066

# Welcome

Located at Fort Lesley J. McNair on the Washington, DC waterfront, the College of Information and Cyberspace (NDU CIC) is one of the five graduate-level colleges that comprise the National Defense University. The CIC educates future thought leaders and change agents who will make the difference in government and strives to meet your workforce education needs for information leadership and management.

## ENROLLMENT PROCEDURES

### Course Registration

Students who are admitted to the CIC at NDU will be sent detailed instructions regarding course registration, account information for online systems, and advisor information. Instructions on how to register for courses through NDU Connect can be found on our website at [Course Registration](#)

### Registration Periods

<b>Semester</b>	<b>Registration Opens</b>	<b>Registration Closes</b>
<b>FALL</b> 14 September 2026 – 6 December 2026	14 June 2026	7 September 2026
<b>SPRING</b> 11 January 2027 – 4 April 2027	14 October 2026	4 January 2027
<b>SUMMER</b> 26 April 2027 – 18 July 2027	15 February 2027	19 April 2027

## COURSE AVAILABILITY IN BLACKBOARD

Each course offering has a site on CIC’s online learning platform, Blackboard. This site will be available to students on the Friday before the Course Start Date. Students must access Blackboard and sign in immediately following the Course Start Date to begin course work. Please note that students will NOT see their course registration in Blackboard until noon on Friday before the course start date.

## DROP POLICY

Students may dis-enroll at any time prior to the Course Start Date (CSD) without a grade recorded on the transcript. In accordance with academic policy, any drop on or after the Course Start Date will result in a grade being assigned in the course. Students who seek to withdraw from a course after the course start date but before the withdrawal period ends will receive a grade of W for the course. Students who seek to withdraw after the withdrawal period end will receive a failing grade for the course. To request to drop a course, students should log into NDU Connect, navigate to course details and select request drop next to the appropriate course.

# Course Models

NDU CIC Fall 2026 *Intensive Courses* will be offered in the following format:  
*Distance Learning.*

## Distance Learning (DL)

The Distance Learning (DL) format engages students and faculty virtually over 12 weeks via Blackboard. Most DLs are asynchronous with a few optional live synchronous sessions weaved in for guest speakers etc., most synchronous sessions will be recorded for students who can’t attend. During the 12 weeks students engage in weekly lessons, assignments and discussion boards. Each course will end with a final assessment which is typically a substantive paper or project that allows students to demonstrate their mastery of the intended learning outcomes. To receive credit for a course, students must be actively engaged virtually in every DL lesson as assigned by faculty.

# Class Schedule by Course

**Please recall that the last day to withdraw from a course with a grade of ‘W’ is:  
Distributed Learning - The Monday of the 4<sup>th</sup> week of class:**

DL	Last Day to Withdraw
14 September 2026 – 6 December 2026	5 October 2026

## CIC – 6422 - Artificial Intelligence Strategies for Data Leaders

This course examines leaders’ roles in the adoption of artificial intelligence (AI) and other data-enabled technologies. Participants explore the technologies, workforce, infrastructure, and other resources necessary to leverage AI within their organizations.

## **CIC-6303 - CIO 2.0 Roles and Responsibilities**

Students in the CIO 2.0 course examine the essential analytic, relational, technological, and leadership competencies that government CIOs and their staff need to respond to and shape the 21<sup>st</sup> Century environment. Students assess the high information and IT demands of customers; examine the potential and perils of ubiquitous technology and information saturation; and weigh the tradeoffs of resource constraints, legal and policy mandates, and security in an open environment.

## **CIC- 6219 - Cyber Essentials for Senior Leaders**

This course focuses on educating senior leaders so that they can better execute the responsibilities of a board member within DOD, Federal Agencies, and international partners. Cyber leaders need both technical knowledge and leadership skills to gain the respect of technical team members, understand what technical staff are doing, and appropriately plan and manage security projects and initiatives. This course empowers the senior leader to become an effective security leader and get up to speed quickly on information security issues and terminology. The content of this is essential for a government senior leader to understand how best to work with the private sector to mitigate the risk of cybersecurity breaches. This course provides the essentials for analyzing the cyber and information security of information systems and critical infrastructures, to include the challenges with cyber legislation and governance, risk management analysis of cyber systems, understanding the cyber threat & vulnerability environments, protecting the organizations intellectual property and financial information and budgeting process. Additionally, participants will have the chance to participate in a tabletop breach exercise and to choose from breakout tracks in healthcare, national security, government oversight, and law.

## **CIC-6177 - Cyber Power and Technology Strategy**

This course examines how the economic instrument of power is applied in the global cyber domain and information environment. Students analyze how state and non-state actors build and project cyber power through technology strategy, fiscal and monetary policy, workforce development, research and development, and commercialization. Emphasis is placed on strategic competition over digital infrastructure, the role of Big Tech in cyber and information operations, deterrence through cyber resilience, and the strategic risks and opportunities of disruptive technologies.

## **CIC-6211 - Cybersecurity Fundamentals**

This course provides an overview of the fundamentals of cybersecurity from the perspective of a DoD or federal agency senior leader. The course provides a foundation for analyzing the cyber and information security of information systems and critical infrastructure. Law, national strategy, public policy, and risk management methodologies are examined for assuring confidentiality, integrity, and availability information systems and asset.

## **CIC-6419 - Data Strategy and Governance**

This course explores data governance as a key component of data strategy for operationalizing data as a strategic asset to enable more effective and efficient decision making. It examines the principles, essential capabilities, and goals set forth in federal agency data strategies and the governance processes necessary to achieve those goals. Case studies allow students to explore the real-world benefits of data governance policies, standards and practices and how they are implemented. The course is designed to provide leaders with knowledge, skills, and attributes to develop and assess data governance programs for their organizations that enable data discovery and sharing and facilitate innovation.

## **CIC-6443 - Emerging and Disruptive Technologies**

This course examines the core concepts of information technology and its rapidly expanding role in solving problems, influencing decision making and implementing organizational changes. Students will be introduced to an array of emerging technologies at various levels of maturity. Students analyze how emerging technologies use qualitative and quantitative evaluation methods. Students assess emerging technologies using forecasting methodologies such as monitoring and experts' opinion, examining future trends, and assessing.

## **CIC-6171 - Governance, Authorities, and Ethics**

This course provides students of national cyber and information strategy with the opportunity to comprehend how information and cyber drive and define nations, their governments, and in turn, their relations in the global context. It is essential that future national security strategists have the capacity to evaluate strategic choices in terms of global and national governance, rights, duties and obligations. Thus, Governance has been developed by crossing leading cyber and information threats, with levels of national and international governance, to identify and examine the key authorities and case studies essential for a future cyber and information strategist. By taking Governance, students will analyze how: law is both a driver and definer of national security strategy; states form and interact through the law; states and private actors use and influence law to pursue vital interests, security, rights, and order; and how future national security strategists and leaders have essential responsibilities to define, engage, and use law when developing national security strategy for cyber and information.

## **CIC-6217 - Illicit Use of Cyber**

This course explores illicit uses of cyber (e.g. terrorism, crime, human trafficking, etc.) and the impact of these activities on national and global security. The course explores the identity of actors engaged in these activities, their motivation, techniques, and what countermeasures can be adopted to mitigate their impact. The course provides a risk management framework to help information leaders leverage the benefits of cyber technologies while minimizing risks.

## **CIC-6151 - Information Warfare Strategy**

This course provides theories, frameworks, and tools for strategic planning and strategy execution. It weds direct and indirect methods of influence. Upon successful completion, students will be able to plan and implement strategies with emphasis on the information instrument of state power in a way that is practical, actionable, and intrepid. These strategies support every warfighting function and all the instruments of state power.

## **CIC-6512 - Multi-Agency Information-Enabled Collaboration**

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

## **CIC-6608 - Risk Management, Internal Controls, and Auditing for Leaders**

This course presents a strategic understanding of risk management, internal controls, and auditing as they relate to the functions and responsibilities within the CFO and audit communities. This course examines how effective leadership can enhance efficiency, effectiveness, accountability, and transparency of an organization to include federal, state, and local governments. The primary focus is on the importance of identifying and assessing risk, describing, and improving internal control techniques and practices, and evaluating and recommending audit management strategies.

## **CIC-6159 - Strategic Art for the Cyber and Information Environment**

In this course, students gain understanding of the origins, formulation, and application of national security strategic logic to the cyber domain and information environment. In so doing, students comprehend their role and duty in the greater tradition of national security strategy; while gaining appreciation of the value they will bring as practitioners of national security strategy for cyber and information. Through the use of readings, case studies, exercises and writing assignments, participants will assess how strategic logic can be used to define context and desired ends, identify necessary means, design ways, and assess costs, risks and viability, with specific focus on the global cyber domain and information environment. Upon completion of NSS, students will be strongly positioned to apply discerning and incisive strategic analysis to their thesis projects, the balance of the courses they will take at CIC and NDU, and in their future careers as professional strategic analysts and leaders.

## **CIC-6415 - Strategic Information Technology Acquisition**

This course explores acquisition processes that seek to place information technology systems into the hands of joint warfighters and agency information leaders faster and with more ability to adapt to fluid situations. We examine the role senior military and agency leaders play in the successful acquisition of information technologies and services to achieve strategic organizational goals. Students use the Systems Development Lifecycle (SDLC) as a framework to explore acquisition strategies and charters, requirements management, development, testing, deployment, risk management and sustainment activities, focusing on the acquisition of IT and related services. Acquisition best practices and techniques cited in the US Digital Services Playbook are explored. IT-related risk management, to include avoidance of counterfeit chips and computer malware, risks of transition to cloud computing and advanced analytics are also discussed. Significant emphasis is placed on the contracting processes and outsourcing of IT

networks and services. Ethics issues are explored using Department of Defense acquisition case studies.

### **CIC-6328 - Strategic Performance and Budget Management**

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

### **CIC-6164 – Strategic Thinking and Communication**

This course provides students with an introduction to graduate-level research, writing, and communication, with a particular focus on the critical and creative thinking that drives strategic decision-making. In support of the NDU and CIC missions, the goal is to enrich strategic thinking and provide support throughout the program for both writing and oral communication. This is the course where students can fully synthesize what they have learned across all their courses and articulate ideas that will help them succeed beyond CIC.

### **CIC-6607 - The Future of Federal Financial Information Sharing**

This course focuses on changing directions of financial and management reporting for Chief Financial Officers in a dynamic environment. In response to evolving citizen and shareholder expectations, financial statement reporting, budgetary reporting, and cash reporting must be accurate, transparent, and accountable, and result in "clean" audit opinions. New reporting expectations and changing accounting standards require new relationships among federal, state, and local governments, and government response to evolving citizen and shareholder expectations, financial statement reporting, budgetary reporting, and cash reporting must be accurate, transparent, and accountable, and result in "clean" audit opinions. New reporting expectations and changing accounting standards require new relationships among federal, state, and local governments, and government contractors, as well as enhanced reporting to internal constituents of the CFO, including program managers and the organizational head. Successful reporting can be facilitated by enterprise architecture, financial systems, and data management techniques.

### **CIC-6606 – White House, Congress and the Budget**

This course presents a strategic understanding of federal budgeting and appropriations, with particular attention to the role of the White House and Congress. The course focuses on developing leadership strategies to shape the fiscal environment to achieve agency strategic outcomes, examining topics such as the impact of current fiscal issues.

## Class Schedule by Date

Course Offering Number	Abbreviation	Section	Course Start Date	On-Site Course Start Date	On-Site Course End Date	Course End Date
CIC-6422_FAL26-27_02	AIS	02	9/14/2026	DL	DL	12/6/2026
CIC-6303_FAL26-27_01	CIO	01	9/14/2026	DL	DL	12/6/2026
CIC-6219_FAL26-27_02	CEL	02	9/14/2026	DL	DL	12/6/2026
CIC-6177_FAL26-27_05	CPT	05	9/14/2026	DL	DL	12/6/2026
CIC-6211_FAL26-27_02	CSF	02	9/14/2026	DL	DL	12/6/2026
CIC-6419_FAL26-27_01	DSG	01	9/14/2026	DL	DL	12/6/2026
CIC-6443_FAL26-27_02	EDT	02	9/14/2026	DL	DL	12/6/2026
CIC-6171_FAL26-27_05	GOV	05	9/14/2026	DL	DL	12/6/2026
CIC-6217_FAL26-27_01	IUC	01	9/14/2026	DL	DL	12/6/2026
CIC-6151_FAL26-27_01	IWS	01	9/14/2026	DL	DL	12/6/2026
CIC-6512_FAL26-27_01	MAC	01	9/14/2026	DL	DL	12/6/2026
CIC-6608_FAL26-27_01	RIA	01	9/14/2026	DL	DL	12/6/2026
CIC-6159_FAL26-27_05	ART	05	9/14/2026	DL	DL	12/6/2026
CIC-6415_FAL26-27_01	ITA	01	9/14/2026	DL	DL	12/6/2026
CIC-6328_FAL26-27_01	SPB	01	9/14/2026	DL	DL	12/6/2026
CIC-6164_AY26-27_05	STC	05	9/14/2026	DL	DL	12/6/2026
CIC-6607_FAL26-27_01	FFR	01	9/14/2026	DL	DL	12/6/2026
CIC-6606_FAL26-27_01	BCP	01	9/14/2026	DL	DL	12/6/2026