
# College of Information and Cyberspace
# Schedule of Courses
# Academic Year 2025-2026
# Spring Trimester

CONTACT DIRECTORY

**INTERNET HOME PAGE**:
http://cic.ndu.edu/

**TELEPHONE:**
202-685-6300
DSN 325-6300

**E-MAIL:**
CICOSS@ndu.edu

**MAILING ADDRESS:**
College Of Information and Cyberspace
Office of Student Services
300 5th 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**

| Semester | Registration Opens | Registration Closes |
|---|---|---|
| **FALL**<br>8 September 2025 – 30 November 2025 | 15 June 2025 | 1 September 2025 |
| **SPRING**<br>12 January 2026 – 5 April 2026 | 15 October 2025 | 5 January 2026 |
| **SUMMER**<br>27 April 2026 – 19 July 2026 | 16 February 2026 | 20 April 2026 |

## 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 Registrar Request, Drop Course Request and select request drop next to the appropriate course.

# Course Models

NDU CIC Spring 2026 *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 4th week of class:**

| DL | Last Day to Withdraw |
|---|---|
| 12 January – 5 April 2026 | 2 February 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. It will familiarize students with the roles and capabilities required to lead, develop, facilitate and employ AI in 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 21st Century environment. Students assess the high information and IT demands of customers; examine the potential and perils of ubiquitous technology and information saturation; and weigh the tradeoffs of resource constraints, legal and policy mandates, and security in an open environment.

## 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 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-6201 – Cyber for Strategic Leaders

This course exercises strategic leadership and critical thinking in the development and use of cybersecurity strategies, plans, policies, enabling technologies, and procedures in cyberspace. It especially explores concepts and practices of strategic thinking and decision-making in leading cyber operations. This course explores network security, threats, vulnerabilities, and risks with the help of specific cases. It analyzes major challenges in cyberspace, assesses specific challenges for cyber leaders, and examines offensive and defensive cyber operations. It provides cyber leaders with an opportunity to explore the intersection of academic and practical, operational knowledge.

## 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-6175 – Cyber Strategy and Conflict

In the contemporary security environment, cyberspace has emerged as a critical domain conflict. State and non-state actors increasingly exploit digital technologies to disrupt critical infrastructure, gather intelligence, influence populations, and contest political, military, and economic power. Events such as Stuxnet, and the persistent activities of groups like Volt Typhoon and Salt Typhoon illustrate how cyber capabilities are used to achieve strategic effects below the threshold of armed conflict. This course examines the evolving character of cyber conflict and its implications for strategy, statecraft, and national security. Through historical cases, theoretical frameworks, and analysis of contemporary operations, students will explore how cyber capabilities are integrated into broader strategies of competition, coercion, and warfare.

## CIC-6420 - Data Analytics for Leaders

This course provides an overview of data analytics concepts and techniques with a focus on what leaders need to know to leverage data for decision making. Students will learn about the data analytics process from the perspectives of both the decision maker and the data analyst to better understand how to build a sustainable data analytics program within a government organization. Topics include analytics approaches, familiarity with data analytics tools, how to determine data requirements, collecting and preparing data, and data ethics. No prior data analytics experience is necessary.

## CIC-6414 – Data Management Strategies and Technologies

This course explores the concepts of data management and the data lifecycle as key components for improving mission effectiveness through the development of enterprise-wide and local data management programs and analytic solutions. It examines management issues such as data governance and organizational information behaviors and values. The course uses the data lifecycle framework to explore big data, data analytics, and enabling information technologies and methodologies from a senior leader perspective. Case studies allow students to explore data management issues and implementation. While geared to managers, the course provides sufficient insight into the underlying technologies to ensure that students can evaluate the capabilities and limitations of data management options and strategies.

## 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-6220 – Engaging Partners and Adversaries through Diplomacy

With a focus on cyberspace and its attendant challenges and opportunities, this course will examine the role of diplomacy in the national security enterprise. Both a U.S. domestic concern and a function of international engagement, diplomacy presupposes a diverse array of actors and interlocutors who may or may not share U.S. interests and values yet with whom policy practitioners must engage to advance U.S. priorities. The course will explore how diplomacy has been used to reduce risk to the US and U.S. interests, and it will consider the capacity of diplomacy to address as-yet- unseen threats to the homeland and the American people. Students will gain

insight into the policy process and how the tools of diplomacy have been used bilaterally and in multilateral forums to advance policy priorities in ways that uphold U.S. principles and values, particularly as they come under threat from strategic competitors and their efforts to undermine U.S. global influence.

## 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- 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

This course focuses on inter-agency collaboration in national, homeland security, and national preparedness planning, decision making, and implementation. It examines current and proposed strategies, means and models for improving inter-agency collaboration at Federal, State, and local levels, and beyond to include multilateral non-governmental and internation organizations and coalition partners.

## 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-6218 – Risk Management Framework for Strategic Leaders

This course prepares future Chief Information Security Officers (CISO), Senior Information Security Officers (SISO) and senior staff involved in the cyberspace component of national military and economic power for their role as an overall cyber risk assessment and acceptance leader. Students explore how cyber security relates to information security, security governance, security program management, system risk assessment and

authorization as well as day-to-day cyber security monitoring management. Students will explore enterprise security strategies, policies, standards, controls, programs, cyber operations, security assessment and measures/metrics, incident response, resource allocation, workforce issues, ethics, roles, and organizational structure.

## 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

## 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 between 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 ID | Course Title | Course Number | Course Abbreviation | Course Start Date | Course End Date |
|---|---|---|---|---|---|
| CIC-6422_SPR25-26_01 | Artificial Intelligence Strategies for Data Leaders | 6442 | AIS | 1/12/2026 | 4/5/2026 |
| CIC-6303_SPR25-26_03 | CIO 2.0 Roles and Responsibilities | 6303 | CIO | 1/12/2026 | 4/5/2026 |
| CIC-6219_SPR25-26_02 | Cyber Essentials for Senior Leaders | 6219 | CEL | 1/12/2026 | 4/5/2026 |
| CIC-6201_SPR25-26_02 | Cyber for Strategic Leaders | 6201 | SEC | 1/12/2026 | 4/5/2026 |
| CIC-6177_SPR25-26_05 | Cyber Power and Technology Strategy | 6177 | CPT | 1/12/2026 | 4/5/2026 |
| CIC-6175_SPR25-26_05 | Cyber Strategy and Conflict | 6175 | CSC | 1/12/2026 | 4/5/2026 |
| CIC-6420_SPR25-26_01 | Data Analytics for Leaders | 6420 | DAL | 1/12/2026 | 4/5/2026 |
| CIC-6414_SPR25-26_01 | Data Management Strategies and Technologies | 6414 | DMS | 1/12/2026 | 4/5/2026 |
| CIC-6443_SPR25-26_03 | Emerging and Disruptive Technologies | 6443 | EDT | 1/12/2026 | 4/5/2026 |
| CIC-6443_SPR25-26_05 | Emerging and Disruptive Technologies | 6443 | EDT | 1/12/2026 | 4/5/2026 |
| CIC-6220_SPR25-26_02 | Engaging Partners and Adversaries through Diplomacy | 6220 | PAD | 1/12/2026 | 4/5/2026 |
| CIC-6171_SPR25-26_06 | Governance, Authorities, and Ethics | 6171 | GOV | 1/12/2026 | 4/5/2026 |
| CIC-6151_SPR25-26_06 | Information Warfare Strategy | 6176 | IWS | 1/12/2026 | 4/5/2026 |
| CIC-6512_SPR25-26_01 | Multi Agency Information Enabled Collaboration | 6512 | MAC | 1/12/2026 | 4/5/2026 |
| CIC-6608_SPR25-26_02 | Risk Management, Internal Controls and Auditing for Leaders | 6608 | RIA | 1/12/2026 | 4/5/2026 |
| CIC-6218_SPR25-26_01 | Risk Management Framework for Strategic Leaders | 6218 | RMF | 1/12/2026 | 4/5/2026 |
| CIC-6159_SPR25-26_06 | Strategic Art for the Cyber and Information Environment | 6159 | ART | 1/12/2026 | 4/5/2026 |
| CIC-6159_SPR25-26_07 | Strategic Art for the Cyber and Information Environment | 6159 | ART | 1/12/2026 | 4/5/2026 |
| CIC-6607_SPR25-26_02 | The Future of Federal Financial Information Sharing | 6607 | FFR | 1/12/2026 | 4/5/2026 |
| CIC-6606_SPR25-26_02 | White House, Congress and the Budget | 6606 | BCP | 1/12/2026 | 4/5/2026 |