Academic Catalog

College of Information and Cyberspace

AY 2023-2024

NATIONAL DEFENSE UNIVERSITY
300 5th Avenue, Building 62, Washington DC, 20319

The College of Information and Cyberspace Academic Catalog is published annually.

The catalog is available online at https://cic.ndu.edu/ under the Academic Catalog tab.

CIC Academic Catalog 2023-2024

The 2023-2024 Academic Catalog of the College and Information and Cyberspace (CIC) provides current information regarding educational programs, class offerings, academic regulations, and university resources. Students can use this document to familiarize themselves with program and degree requirements relevant to their degree or certificate program.

Statements in this catalog should be treated as solely informational. This document should not be construed as binding between the student and the university. While every effort is made to keep the Academic Catalog updated, CIC reserves the right to amend policies and procedures as it sees fit. Every effort will be made to communicate any alterations.

NDU CIC is an equal opportunity institution. The College is committed to providing equal education and employment opportunities to qualified persons while ensuring freedom from discrimination or harassment of any kind. Equity, diversity, and inclusion are principles fundamental to our productivity and effectiveness. Supervisors and employees will adhere to all Equal Employment Opportunity and Equal Employment policies and regulations.

Information in this catalog is accurate at the date of publication. Please consult the website for recent updates.

Table of Contents

As of 06 September 2023

Mission

College of Information Cyberspace educates joint warfighters, national security leaders, and the cyber workforce on the cyber domain and information environment to lead, advise, and advance national and global security.

Vision

CIC is the premier senior national security educational institution focused on the information environment. CIC is the desired educator of leaders who perform national and military actions within the cyberspace domain using the information instrument of national power.

Letter from the Chancellor

It is my immense pleasure to welcome you to Academic Year (AY) 2023-2024 at the National Defense University's College of Information and Cyberspace (CIC). Our college, faculty, and staff are committed to making your educational journey at CIC one of the best academic experiences available. CIC sets the standard for education and remains the preeminent institution for cyber and information education within the Department of Defense and the United States Government. In AY23-24 we will continue to meet and exceed that standard.

During AY22-23, the college experienced a record enrollment, and we were thrilled to welcome world-class scholars and faculty with a range of military, government, academic, and industry experience. CIC faculty continued to demonstrate innovation and leadership in their respective fields.

Dr. Gwyneth Sutherlin launched a two-year project funded by an OSD Minerva grant to examine cultural variation in artificial intelligence using cognitive linguistics, and Dr. Jill Goldenziel selected as a member of the Executive Council of the American Society of International Law in recognition of exceptional contributions to the field. Dr. Joseph Schafer, the recipient of the first-ever CIC Research Sabbatical. CIC also hosted six esteemed visiting faculty members from the Department of Energy, Department of State, Defense Information and Systems Agency, the Department of Homeland Security, the Federal Accounting Standards Advisory Board, and US Cyber Command.

For the first time since 2020, CIC "Ravens" took part in academic field studies, a vital part of our on-campus academic programs: CIO-LDP students traveled throughout the DC and NYC areas, and the JPME II cohorts visited NYC and either the UK or Belgium and Estonia. CIC also convened the ninth annual Cyber Beacon symposium, which featured keynotes from former Representative Jim Langevin and Robert Knake, the Deputy National Cyber Director for Strategy and Budget. The college also partnered with U.S. Cyber Command to host their annual CYBERCOM Symposium, with a keynote address and attendance from its Commander, General Paul Nakasone.

Of further note, we inaugurated our first Cyber Leadership Development Program. This Program is focuses on the integration of cyberspace and national security providing a deeper understanding of how effective leadership in the cyber domain is pivotal to the success of U.S. and international security. The National Advisory Committee on Institutional Quality and Integrity (NACIQI) voted to recommend to the Department of Education CIC's degree name change from Government Information Leadership to Strategic Information and Cyberspace Studies.

Our faculty, staff, conferences, and meeting all focus on supporting our stakeholders and you, our students. We hope you will use your time at CIC to collect valuable knowledge, tools, frameworks, relationships, and experiences. Consider this educational experience an opportunity to gain experience, reflect, and practice, in order that you may leave CIC prepared to be the kind of thoughtful, principled leader needed by the United States, its partners, and its allies.

Dr. Cassandra Lewis
Chancellor
College of Information and Cyberspace

CIC Overview

The College of Information and Cyberspace (CIC) offers a wide spectrum of educational activities, services, and programs which prepare leaders to play critical roles in national security. Through our Master of Science, certificates, and professional development opportunities—CIC students are molded into lifelong learners, effective communicators, and dynamic thinkers. Students, alumni, faculty, and staff constitute one of the premier global learning communities in the fields of information and cyberspace.

Government Information Leadership - Master of Science Degree[1]

Overview

The Master of Science Degree aligns with the educational requirements of the DoD cyber workforce in support of national strategies, policies, laws, and directives. The 10-month in-residence program achieved Joint Staff (JS) Process for Accreditation of Joint Education (PAJE) approval in 2019. The College is in the process of recertifying as a National Security Agency Center for Academic Excellence. Additionally, CIC maintains Memoranda of Agreement with over 30 civilian colleges and universities to facilitate student transfer credit and completion of the DoD Cyber Scholarship Retention Program.

Modalities

- Full time In-residence (10-months, Fall and Spring semesters)—U.S. Military Selectees earn Joint Professional Military Education, Phase II (JPME II)
- Part-time Hybrid (Online and In-residence)

Program Learning Outcomes

- Evaluate the national security environment with a focus on the informational instrument of power and cyberspace.
- Create information policy, strategy, and campaign plan options that support joint warfighting and achieve national security objectives.
- Create cyber policy, strategy, and campaign plan options that support joint warfighting and achieve national security objectives.
- Analyze the ethical, legal, and policy implications of emerging and disruptive technologies on the changing character of war.
- Apply principles of strategic leadership to include effective communication, creative and critical thinking, decision making, and ethical conduct.

[1] The MS Degree program is currently titled Government Information Leadership (GIL), But will be renamed to Strategic Information and Cyberspace Studies upon final approval from the Department of Education

Master of Science GIL In-residence/JPME (36 Credit Hours)

Core Courses 30 Credit Hours (CH)
Foundations of the Information Environment
Governance of the Global Information Environment and Cyber Domain
Information Warfare Strategy
International Challenges in Cyberspace
National Security Strategy
Practicum, Experiential Learning and Capstone Exercise
Strategic Competition in the Information Environment
Strategic Leader Foundational Course
Strategic Thinking and Communication
Warfighting and Disruptive Technologies
Three NDU Electives*

* NDU elective are 2 Credit Hours each offered to resident master's students by CIC and the other NDU colleges.

Master of Science GIL Part-time (36 Credit Hours)

Core Courses 30 Credit Hours (CH)
Emerging and Disruptive Technologies
Foundations of the Information Environment
Governance of the Global Information Environment and Cyber Domain
Information Warfare Strategy
International Challenges in Cyberspace
National Security Strategy
Strategic Competition in the Information Environment
Strategic Leader Foundational Course
Strategic Thinking and Communication
Cyber Elective
Two CIC Electives **

** CIC electives for the MS are 3 Credit Hours each, student may select any courses from the CIC course catalog to meet the MS elective requirement.

Chief Information Officer Leadership Development Program

Overview

The Chief Information Officer Leadership Development Program (CIO-LDP) is the CIC's flagship resident program for rising senior-level managers and leaders responsible for promoting and attaining national and international security goals through the strategic use of information and information technology as identified in the CIO competencies. The CIO-LDP is administered in an intensive and highly interactive fourteen-week forum. The student- centered educational experience emphasizes developing leadership skills and abilities while learning CIO content through completion of five courses. Students who complete the program will receive a CIO graduate certificate.

Modalities

- Full time In-residence (14 weeks)

Program Learning Outcomes

- Leverage CIO policy and organization competencies to lead within and across federal organizational boundaries by linking critical decisions regarding resources, people, processes, and technologies to mission performance.
- Balance continuity and change in the development implementation, and evaluation of government information resources and management strategies and policies while meeting legislative and executive mandates.
- Demonstrate abilities to construct and implement mission-aligned information and communication technology strategies [including gathering, analyzing, and reporting data; making decisions; implementing decisions; and evaluating organizational performance] in an ethical manner.
- Communicate at the strategic level demonstrating command of the topic, logical organization, compelling argument, and excellence in English grammar and syntax.

Core Courses (15 Credits)
CIO 2.0 Roles and Responsibilities
Strategic Performance and Budget Management
Strategic Information Technology Acquisition
Emerging and Disruptive Technologies
Cybersecurity Fundamentals

Cyber Leadership Development Program

Overview

The Cyber Leadership Development Program (Cyber-LDP) prepares students to meet rapidly expanding cyber competencies and effectively integrate elements of cyberspace with national strategy. Courses emphasize current and evolving leadership, management direction, and advocacy to manage cybersecurity risk in this constantly evolving domain. Students will face rigorous case studies and scenarios to develop their skills in partnering, strategic thinking, team building, problem solving, and negotiating on current and emerging technologies. Threats in cyberspace are constantly evolving and this program provides students the opportunity to explore solutions in the context of public-private partnerships and challenge the status quo. This program is ideal for students who are currently or projected to be in the National Institute of Standards and Technology (NIST) Workforce Framework for Cybersecurity (NICE) Work Roles in Oversight and Governance or equivalent to enhance and gain competencies. Students who complete the intensive receive a Cyber Leader certificate.

Modalities

- Full time In-residence (14 weeks)

Program Learning Outcomes

- Mature an understanding of the cyber threat landscape to include projections for the future to develop a strategic approach to cyberspace activities that incorporates the USG and partnerships with domestic and international partners.
- Apply key strategic concepts, critical thinking, and analytical frameworks to the analysis of national and international security environments in support of formulating, implementing, and evaluating national security, cyber strategy, and statecraft to enable mission success.
- Assess emerging technologies using forecasting methodologies such as monitoring and expert opinion, examining future trends, and assessing international perspectives to develop policy and ensure future mission capabilities.
- Identify, evaluate, and counter major cyber threats and threat actors and ways the U.S. and international community can leverage bilateral and multilateral mechanisms to counter threats as technology rapidly evolves.
- Apply critical, strategic, ethical, and innovative thinking to lead organizations in an increasingly vulnerable technology dependent world.

Core Courses (15 Credits)
Cyber Essentials for Senior Leaders
Cyberspace Activities and Authorities
Emerging and Disruptive Technologies
Emerging Partners and Adversaries through Diplomacy
National Security and Cyber Strategy

CIC Graduate Certificates

The CIC Graduate Certificates support the educational requirements of the DoD cyber workforce with focused coursework. Students may apply a maximum of three courses (9 CH) from certificates programs to the MS degree whether these courses are electives or core courses. A course can only be used once to meet a certificate requirement, students must take an alternative course to meet program requirements.

Chief Data Officer (CDO) Graduate Certificate

Modalities

- Hybrid (part-time, including online and in-residence components)
- Distance (Online)

Certificate Learning Outcomes

- Apply data analytics tools and methodologies on data sets and communicate results with impactful visualizations.
- Advocate and communicate date sharing practices through organizational culture, policies, and systems development process while fulfilling legal and ethical obligations of data ownership.
- Evaluate enabling technologies and enterprise/data architectures to address requirements for data analytics programs, including real-time Big Data processing and machine learning/predictive analytic capabilities.
- Create a data analytics program through data governance initiatives that support all data life-cycle considerations (e.g., authoritative, source consolidation, updating, purging/avoiding sprawl, and archival).
- Employ the emerging technologies (and underlying data) to enhance data-driven decision-making for strategic effect.
- Identify, shape, and formulate data strategies that ensure data availability and transparency, supporting multi-agency and/or multi-national collaboration.

Chief Data Officer Certificate (5 courses—15 Credits)

Core Courses (15 Credits)
Data Management Strategies and Technologies: A Managerial Perspective
Strategic Information Technology Acquisition
Data Analytics for Decision Makers
Emerging and Disruptive Technologies
Data Strategy and Governance

Chief Financial Officer (CFO) Graduate Certificate

Modalities

- Hybrid (part-time, including online and in-residence components)
- Distance (Online)

Certificate Learning Outcomes

- Lead within and across organizational boundaries by leveraging knowledge of federal budgeting, financial accounting and reporting, data management and analytics, risk, internal controls, and audit for strategic advantage.
- Synthesize ethics, theory, practices, and technologies to promote effective decision-making and accountability across the enterprise, improve operations, and support financial management excellence.
- Communicate at the strategic level, demonstrating command of the topic, logical organization, compelling argument, and excellence in English grammar and syntax.

CFO Certificate (5 courses—15 Credits)

Core Courses (15 Credits)
Strategic Performance and Budget Management
Data Management Strategies and Technologies: A Managerial Perspective
White House, Congress, and Budget
The Future of Federal Financial Information Sharing
Risk Management, Internal Controls and Auditing for Leaders
Alternate Courses:
Strategic Information and Technology Information

Chief Information Officer (CIO) – Graduate Certificate

Modalities

- Hybrid (part-time, including online and in-residence components)
- Distance (Online)

Certificate Learning Outcomes

- Leverage CIO policy and organization competencies to lead within and across federal organizational boundaries by linking critical decisions regarding resources, people, processes, and technologies to mission performance.
- Balance continuity and change in the development, implementation, and evaluation of government information resources and management strategies and policies while meeting legislative and executive mandates.
- Demonstrate abilities to construct and implement mission-aligned information and communication technology strategies, including gathering, analyzing, and reporting data; making decisions; implementing decisions; and evaluating organizational performance in an ethical manner.
- Communicate at the strategic level demonstrating command of the topic, logical organization, compelling argument, and excellence in English grammar and syntax.

CIO Graduate Certificate (5 courses—15 Credits)

Core Courses (15 Credits)
CIO 2.0 Roles and Responsibilities
Strategic Performance and Budget Management
Strategic Information Technology Acquisition
Emerging and Disruptive Technologies
Cybersecurity Fundamentals
Alternate Courses:
Data Management Strategies and Technologies: A Managerial Perspective
Capital Planning and Portfolio Management

Chief Information Security Officer (CISO) Graduate Certificate

Modalities

- Hybrid (part-time, including online and in-residence components)
- Distance (Online)

Certificate Learning Outcomes

- Exercise strategic leadership and critical thinking in the development and use of cyber security strategies, plans, policies, enabling technologies and procedures in cyberspace.
- Develop and lead programs to provide cyber security, security awareness training, risk analysis, certificate and accreditation, security incident management, continuity of operation and disaster recovery.
- Link people, processes, information, and technology to critical cyber mission decisions to share information in a secure environment.
- Develop and lead, in accordance with laws and regulations, an enterprise IA program that promotes and attains national security, agency, and inter-agency goals.
- Communicate at the strategic level demonstrating command of the topic, logical organization, compelling argument, and excellence in English grammar and syntax.

CISO Certificate (5 courses—15 Credits)

Core Courses (15 Credits)
Cybersecurity Fundamentals
Cyber Security for Information Leaders
Illicit Use of Cyber
Risk Management Framework for Strategic Leaders
Critical Information Infrastructure Protection or Continuity of Operations

Cyber Leadership Graduate Certificate

Modalities

- Hybrid (part-time, including online and in-residence components)
- Distance (Online)

Certificate Learning Outcomes

- Mature an understanding of the cyber threat landscape to include projections for the future to develop a strategic approach to cyberspace activities that incorporates the USG and partnerships with domestic and international partners.
- Apply key strategic concepts, critical thinking and analytical frameworks to the analysis of national and international security environments in support of formulating, implementing and evaluating national security, cyber strategy, and statecraft to enable mission success.
- Assess emerging technologies using forecasting methodologies such as monitoring and expert opinion, examining future trends, and assessing international perspectives to develop policy and ensure future mission capabilities.
- Identify, evaluate, and counter major cyber threats and threat actors and ways the U.S. and international community can leverage bilateral and multilateral mechanisms to counter threats as technology rapidly evolves.
- Apply critical, strategic, ethical, and innovative thinking to lead organizations in an increasingly vulnerable technology dependent world.

Cyber Leadership Certificate (5 courses—15 Credits)

Core Courses (15 Credits)
Cybersecurity Fundamentals
Illicit Use of Cyber
National Security Strategies
Multi-Agency Information-Enabled Collaboration
Cyberlaw
Alternate Courses:
Critical Information Infrastructure Protection
Emerging and Disruptive Technologies

Information Technology Program Management Graduate Certificate

Modalities

- Hybrid (part-time, including online and in-residence components)
- Distance (Online)

Certificate Learning Outcomes

- Lead and manage complex IT acquisition and other projects and programs that create value for the organization through enhanced mission performance.
- Apply higher order skills in critical thinking, negotiation, collaboration, and persuasion to synthesize solutions to program management challenges within and across organizational boundaries in an ethical manner.
- Identify ways to use innovative technologies to accomplish customer service activities, thereby lowering costs, decreasing service delivery times, and improving the customer experience.
- Evaluate the organizational value of new information technologies and develop strategies for employing them for strategic advantage.
- Communicate at the strategic level demonstrating command of the topic, logical organization, compelling argument, and excellence in English grammar and syntax

ITPM Certificate (5 courses—15 Credits)

Core Courses (15 Credits)
Capital Planning and Portfolio Management
Information Technology Program Leadership
Data Management Strategies and Technologies: A Managerial Perspective
Strategic Information Technology Acquisition
Information Technology Project Management

Non-Program Seeking

Non-program seeking status allows students who meet College of Information and Cyberspace (CIC) program eligibility requirements to enroll in courses without declaring an intent to complete a particular CIC program. Students may take up to 9 credits before they must select a program. All courses must be taken for a letter grade and will be recorded on student academic transcripts. Completed courses with grades of B or higher may be applied to the applicable requirements of the selected program.

Course Descriptions

Capstone 6700 (CAP) [part time only]

The Capstone course is the culminating learning experience of the Government Information Leadership (GIL) Master of Science Degree Program. While enrolled in CAP, students complete a Capstone synthesis project in their area of concentration. The NDU CIC department responsible for each Master of Science concentration will define the specific nature and detailed requirements for the type of project suitable for the respective concentration and decide how a particular project type is assigned to a specific student.

Continuity of Operations 6504 (COO)

This course provides a broad description of the major elements involved in developing and implementing effective Continuity of Operations plans for public sector agencies. Using Federal regulations and policies as a backdrop, the course examines the technological, human capital, legal, and acquisition factors involved in creating and maintaining a COOP 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.

CIO 2.0 Roles and Responsibilities 6303 (CIO)

Students in the CIO 2.0 course examine the essential analytic, relational, technological, and leadership competencies that government CIOs and their staffs 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.

Critical Information Infrastructure Protection 6230 (CIP)

This course examines the security of information in computer and communications networks within infrastructure sectors critical to national security. These include banking, securities and commodities markets, industrial supply chain, electrical/smart grid, energy production, transportation systems, communications, water supply, and health. Special attention is paid to the risk management of information in critical infrastructure environments through an analysis and synthesis of assets, threats, vulnerabilities, impacts, and countermeasures. Students learn the importance of interconnection reliability and methods for observing, measuring, and testing negative impacts. Special consideration is paid to the key role of Supervisory Control and Data Acquisition (SCADA) systems in the flow of resources such as electricity, water, and fuel. Students will learn how to develop an improved security posture for a segment of the nation's critical information infrastructure.

Cyber Essentials for Senior Leaders 6219 (CEL)

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.

Cybersecurity Fundamentals 6211 (CSF)

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 the confidentiality, integrity, and availability information systems and asset.

Cyberspace Activities and Authorities 6221 (CAA)

This course focuses on authorities across US Agencies and international bodies regarding cyber activities to include but not limited to: security, defense, exploitation, and attack. According to the National Cybersecurity Strategy 2023: "Our rapidly evolving world demands a more intentional, more coordinated, and more well-resourced approach to cyber defense. We face a complex threat environment, with state and non-state actors developing and executing novel campaigns to threaten our interests." This course explores how the US to include government, law enforcement, and industry, working with allies and partners, use all instruments of power to disrupt and dismantle threat actors to US national security interests.

Cyber Security for Information Leaders 6201 (SEC)

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.

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

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 for managers, the course provides sufficient insight into the underlying technologies to ensure that students can evaluate the capabilities and limitations of data management options and strategies.

Emerging and Disruptive Technologies 6443 (EDT)

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

international perspectives.

Engaging Partners and Adversaries through Diplomacy 6220 (EPA)

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.

Foundations of the Information Environment 6165 (FIE)

This course introduces and explores the foundational concepts of cyberspace as a component of the information environment. We first examine the information environment -- the physical, virtual, and human aspects — in order to understand how and why our actions have strategic value. Then we consider the actions themselves from the technical and human perspective, with particular focus on information-related capabilities and activities in and through cyberspace, in order to understand how to deploy them. Finally, we learn about how to generate, acquire, and manage the resources for cyber and information operations.

Future of Federal Financial Information Sharing 6607 (FFR)

This course focuses on the 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.

The Governance of the Information Environment and Cyber Domain 6171 (GOV)

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.

Illicit Use of Cyber 6217 (IUC)

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.

Information, Warfare, Strategy 6151 (IWS)

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.

International Challenges in Cyberspace 6154 (ICC)

This course is designed to provide students with an overview of the issues surrounding cyberspace, including global governance and policy frameworks, international investment, and other national policies relevant to cyberspace. Students will be introduced to the goals and perspectives of critical state and non-state actors aswell as social, political, economic, and cultural factors that lead to diverse international perspectives to better understand how the US and allied states should formulate strategy and policy for cyberspace.

Multi-Agency Information-Enabled Collaboration 6512 (MAC)

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 international organizations and coalition partners.

National Security and Cyber Strategy 6330 (NCS)

The Course is primary strategy course of the CIC Cyber Leader Development Program. Students gain understanding of the origins, formulation, and application of national security strategic logic to the cyber domain and information environment. Further, students will examine and learn the implications for subordinate organizations of the latest National Cyber Strategy. 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. 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.

National Security Strategy 6159 (NSS)

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 take at CIC and NDU, and in their future careers as professional strategic analysts and leaders.

Risk Management for Senior Leaders 6218 (RMF)

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.

Risk Management, Internal Controls, and Auditing for Leaders 6608 (RIA)

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.

Strategic Competition in the Information Environment 6166 (SCIE)

In this course, students will analyze how information and cyberspace operations are integrated into joint warfare and theater campaign strategies. Students will explain what is needed to operationalize information and cyber power for theater strategy and campaigning using joint planning systems and processes. Finally, students will create and propose military actions for campaigns, operations, and activities in the Information Environment and Cyberspace to achieve strategic and operational objectives.

Strategic Information Technology Acquisition 6415 (ITA)

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 Life-cycle (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.

Strategic Leader Foundation Course 6168 (SLF)

Welcome to the Strategic Leadership Foundational Course (SLFC). The purpose of the course is to provide students with a common intellectual foundation essential for success in the College of Information and Cyberspace curriculum and longer-term success as senior leaders. The course will provide a foundation to develop the skills for creative and critical thinking; explore the concepts, principles, and skills to help understand the global security environment and address the challenges of strategic leadership; introduce students to the Joint Force and the strategic aspects of Joint Professional Military Education; and provide a foundation in information theory and strategic principles. The course contains four sections that work together to achieve the desired learning outcomes: I) Strategic Leader Critical Thinking, II) Strategic Documents and Key Joint Professional Military Education Learning Objectives, III) Sovereignty, Interests, and Grand Strategy, and IV) Information Theory and Power.

Strategic Performance and Budget Management 6328 (SPB)

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.

Strategic Thinking and Communication 6414 (STC)

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 the ideas that will help them succeed beyond CIC.

White House, Congress, and Budget 6606 (BCP)

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.

Colleges and Universities Accepting CIC Credits

CIC maintains academic partnerships with regionally accredited universities whose degrees align well with our academic vision and educational programming. Graduates from our certificate programs can apply to several partner institutions for completion of a master's or doctoral degree program.

Academic partners generally accept 9-12 graduate semester credits dependent on the certificate program, and the number of courses completed with CIC. Students enrolled in CIC programs prior to mid-2014 may receive up to 15 transfer credits, depending on the certificate program.

We currently have 29 partner institutions. Many partners provide full-time, part-time, and/or online learning opportunities. Several CIC partner universities updated their agreements over the previous year to include new degrees and acceptance of additional NDU CIC certificates. Please check our website for an updated list: https://cic.ndu.edu/catalog/partners/.

Questions about CIC's Academic Partners, or the Academic Partner Program more broadly, should be directed to Joe Billingsley, Director of Strategic Engagement (+1.202.685.2020).

Auburn (AL)	Cal State San Bernardino (CA)
Capitol Technology University (MD)	Central Michigan University (MI)
East Carolina University (NC)	Florida Institute of Technology (FL)
Fort Hayes State University (KS)	George Mason University (VA)
Global IA Certification (GIAC)	SANS Illinois Institute of Technology (IL)
James Madison University (VA)	Johns Hopkins University (MD)
Missouri Univ. of Science and Technology (MO)	New Jersey City University (MJ)
New Mexico Tech (NM)	Northeastern University (MA)
Nova Southeastern University (FL)	Pace University (NY)
Regis University (CO)	San Diego State University (CA)
Southern Methodist University (TX)	Syracuse University (NY and DC)
University of Arkansas at Little Rock (AR)	University of Detroit Mercy (MI)
University of Illinois at Springfield (IL)	University of MD Baltimore County (MD)
University of MD Global Campus (MD)	University of Nebraska at Omaha (NE)
University of North Carolina at Charlotte (NC)	University of Texas at San Antonio (TX)
University of Tulsa (OK)	University of Washington (WA)
Walsh College (MI)	

(As of July, 2022)

Cyber PME Consortium

The Cyber Professional Military Education (PME) Consortium is a structured community of interest led by CIC. It was born out the demand for increased collaboration among the many educators and trainers focused on cyber topics across the American PME community. In addition to online resource sharing and discussion, physical meetings have taken place at CIC and rotating hosts like the Air Cyber Collage and Naval War College. Updates about this Consortium can be found here, https://cic.ndu.edu/Events/Cyber-PME-Consortium/.

DoD University Consortium for Cybersecurity Coordination Center (UC2)

CIC serves as the Coordination Center for the DoD University Consortium for Cybersecurity (UC2). The UC2 Director is Dr. Gwyneth Sutherlin.

UC2 fulfills the legislative requirement of the 2020 National Defense Authorization Act (NDAA) Section 1659 (Consortia of Universities to Advise Secretary Defense on Cybersecurity Matters). UC2 exists to facilitate the two-way communication between the Secretary of Defense (SECDEF) and academia across the United States.

Key partners of this effort include the National Security Agency (NSA) Center of Academic Excellence (CAE) Community and the Office of the Under Secretary of Defense (USD) for Research and Engineering (R&E).

Admissions

Minimum Eligibility Criteria

1. U.S. Government Affiliation
    a. Federal Government civilian employees, military officers, non-federal government employees (state and local government), and private sector employees working in a field relevant to the CIC curriculum and approved by the joint staff.
2. Education
    a. All applicants must possess a bachelor's degree from a regionally accredited U.S. institution or the equivalent from a foreign institution. The minimum grade point average considered for admission is a 3.0 on a 4.0 scale for all previous undergraduate work. In cases where the undergraduate GPS is below 3.0, a cumulative GPA of 3.3 in 6 or more graduate credits (from CIC or other accredited programs) may be used to determine eligibility.
3. Pay Grade/Rank and Experience
    a. A federal civil service pay grade of GS-13 or equivalent/military officer rank of O-4 or above. Non-federal employees, to include state and local government, must be of an equivalent grade. Private sector employees must be of an equivalent grade and work in a field relevant to the CIC curriculum.
4. English Language Proficiency (if necessary)
    a. International students whose native language is not English are required to demonstrate their English proficiency by passing an English comprehension test with an ECL of 85 for the CIO Leadership Development Program or a 90 for all other certificate programs. Exceptions can be made for applicants whose university degree is from a regionally accredited U.S. institution, or whose home country is on the DSCA Country Exemption List. Contact the CIC Office of Student Services for further details.

Military Reserves and National Guard

Members of the Military Reserves or National Guard who do not meet the above admissions criteria (e.g., Government affiliation) may apply for admission based on their full-time Military Reserve or National Guard status. Education and grade/rank minimum requirements apply regardless of employer. Contact the CIC Office of Student Services for further details.

International Applicants

International students (non-US citizens) must apply through the appropriate Security Assistance Training Field Activity (SATFA) country program manager. For additional information, please visit the CIC international student's webpage at https://cic.ndu.edu/Admissions/International-Students/.

Applications for Admission

A. Required documents for Master's and Leadership Development Programs:

1. Application for Admission
2. Résumé
3. Employment Verification and Recommendation Form
4. Professional Letter of Recommendation
5. Official Undergraduate and Graduate (if applicable) Transcript(s)
6. Writing Sample

B. Required documents for Certificate and Non-Program Seeking:

1. Application for Admission
2. Résumé
3. Employment Verification and Recommendation Form
4. Official Undergraduate and Graduate (if applicable) Transcript(s)

For further information, please refer to our instructions online at https://cic.ndu.edu/Admissions/Application-Instructions/.

To Apply

U.S. applicants should submit all the required documents in the same application packet online at https://cic.ndu.edu/Admissions/Apply-Online/. International applicants, please see previous section on international student enrollment for SATFA guidance.

Mail official transcripts to:
NDU CIC Office of Student Services
300 5th Avenue, Marshall Hall, Building 62, Room 145
Fort McNair, Washington, DC 20319

Email official transcript to:
CICOSS@ndu.edu

Admissions Deadlines

All Certificate, Non-Program Seeking, M.S. degree, and CIO-LDP programs are open to new applicants and existing CIC students.

Certificate, Non-Program Seeking, and M.S. degree applications are reviewed on a rolling basis. For admission to a specific term, please provide a complete application, including all supplemental materials, no later than the dates listed below:

Spring 2024 Semester: September 1, 2023
Summer 2024 Semester: January 1, 2024
Fall 2025 Semester: June 1, 2024

Please note that all courses are taken for graduate credit. Thus, all students are required to be admitted to a program prior to registering for a course. Please complete the admissions process before submitting a course request.

NDU CIC courses are available to eligible Federal civilian agency government employees, Department of Defense (DoD) civilian employees, military officers, non-Federal Government employees (i.e. state and local government), and private sector employees sponsored by a government agency.

Program Policies

All students are responsible for understanding the academic policies of the university and their academic program, including deadlines, attendance, curriculum requirements, grades, and academic integrity.

Applying Coursework from Other Institutions

Graduate Certificate Program Participants

CIC does not accept transfer credits from outside institutions. CIC courses taken for non-credit may not be used to fulfill certificate requirements. Courses that cross certificates may only be used to fulfill one certificate requirement; in these cases, an alternate course will be identified for program completion. All coursework applied toward a certificate must be completed within four years of program admission.

Master of Science Program Participants

Subject to graduate time limit requirements, a student may use up to three NDU CIC classes passed with a grade of B or higher toward attaining the Master of Science degree. Courses from outside institutions are not accepted for transfer. CIC courses taken for non-credit may not be used to fulfill certificate requirements. All coursework applied toward the Master of Science degree must be completed within five years of program admission.

Leave of Absence

Students may apply for a leave of absence due to exceptional circumstances by submitting a written

request to NDU CIC Office of Student Services. The letter should provide a detailed explanation of the circumstances leading to the request, and a justification of the time requested. Requests for a leave of absence may be made for up to one academic year. An approved leave of absence will extend the student's program completion timeline. Requests should be e-mailed to CICOSS@ndu.edu. Approval will be provided by e-mail.

Program Withdrawal

Students seeking to withdraw from NDU CIC programming must submit the program withdrawal form found on our website https://cic.ndu.edu/catalog/policies/to NDU CIC Office of Student Services. Confirmation of withdrawal will be provided via email.

Continued Enrollment

Students must demonstrate continued progress at NDU CIC to maintain enrollment. This requires a minimum of one course every 12 months, and a cumulative 3.0 overall GPA. Students who fail to meet these standards will be administratively withdrawn from the college. Students are eligible to reapply for admission.

Master of Science (M.S.) Degree Program: All coursework applied toward a M.S. Degree must be completed within five (5) years of program admission. Courses taken after the five-year deadline will be subject to repeat, although the credit itself will not be revoked.

Graduate Certificate Programs: All coursework applied toward a certificate must be completed within four (4) years of program admission. Courses taken after the four-year deadline will be subject to repeat, although the credit itself will not be revoked.

Academic Probation

Students will be placed on probation upon receiving one (1) course grade of F and/or when their cumulative GPA falls below the required 3.0 for continued enrollment. Students on probation must attend a mandatory counseling session with their academic advisor and, if applicable, raise the GPA to a 3.0 on a timeline approved by the NDU CIC Office of the Dean. Students who receive a second course grade of F and/or who fail to raise their GPA within the prescribed timeline or credit load will be dismissed from the program.

Dismissal

CIC may dismiss students from the program for reasons including, but not limited to, unsatisfactory academic progress/performance, and/or upon the decision of the Academic Review Board.

Reinstatement

Dismissed students who wish to seek reinstatement must reapply for program admission. CIC may grant reinstatement on a case-by-case basis. Once eligibility is reviewed, it will be determined which

previous courses, if any, may apply to the reinstated student's body of study.

Academic Policies

Student Preparation

Students are expected to prepare for each academic session by reading assigned materials. Readings are often the focus for seminar discussions, or key parts of in-class exercises. Faculty and other seminar participants will assume that reading assignments have been completed by the start of the session.

Student Assessment

CIC students must demonstrate mastery of intended learning outcomes in each course. Faculty members formally assess student achievement of learning outcomes as detailed in course assessment plans and provide detailed feedback to students on their performance. Faculty members utilize assessment plans highlighting proposed assessment techniques, including but not limited to papers, projects, exercises, and participation. CIC end-of-course assessments require students to apply the material through written papers or presentations. End-of-course assessments submitted for a grade cannot be rewritten or resubmitted.

Grading

The following letter grades and their achievement equivalents are used by the NDU CIC to evaluate student performance in courses and in the overall program. Grade points corresponding to each letter grade determine a student's academic average and eligibility to graduate. Master of Science and Graduate Certificate students must maintain a GPA of at least 3.0 to graduate.

Only one grade of C may be used to fulfill certificate program requirements, while a grade of C cannot be used to fulfill requirements for the Master of Science degree program.

NDU Grade Scale

The table below shows letter grades, qualitative descriptors, quality points, and percent ranges to be used for grading. While brief, the While brief, the qualitative grade descriptors nonetheless capture the range of graded outcomes, with the grade of B+ generally associated with the expected student performance. Quality points are used to calculate a student's Grade Point Average (GPA), whereas percent ranges are used for final course grades, individual assignments, and other course activities. Course letter grades and overall GPA are displayed on the student's transcript.

Letter Grade	Qualitative Descriptor	Quality Points	Percentage Range	Point Range for Rounding
A	Excellent (or Top tier) Performance	4.00	96-100	95.50-100.00
A-	Better than Expected Performance	3.70	90-95	89.50-95.49
B+	Expected Level of Performance	3.30	86-89	85.50-89.49
B	Acceptable Performance	3.00	83-86	82.50-85.49
B-	Marginal Performance	2.70	80-82	79.50-82.49
C	Unacceptable Performance	2.00	70-79	69.50-79.49
F (For graded course)	Failure	0.00	0-69	0.00-69.49
P (For Pass-Fail designated course)	Pass	0.00	N/A	N/A
F (For Pass-Fail designated course)	Fail	0.00	N/A	N/A

Non-GPA Annotations

Non-Credit Bearing Audit: The audit grade is assigned to students who elect to take a course for non-credit. Audit is awarded to students who successfully complete requirements except the final assessment. To attain full academic credit, students must retake the course. Students must declare, in writing, if they are taking the course for non-credit by Friday of the seminar week (week 2).

Incomplete (I) The I grade for a course will be assigned only upon approval of the course instructor and the Dean of Faculty and Academic Programs. Incomplete indicates that one or more course requirements has not been completed for reasons that, in the judgment of the course director, were unavoidable. A student must initiate the request for an incomplete grade with the instructor. The student and the instructor will specify in writing the requirements to be completed and the deadline for completion, which may not exceed two semesters. Upon completing all the outstanding requirements, the student must request that the instructor change the Incomplete to the appropriate letter grade. Any Incomplete grade not resolved within two semesters will be automatically converted to an F grade.

Course Withdrawal (W):

Students who drop a course on or after the Course Start Date (CSD) but before 25 percent of the course is completed will receive an academic grade of W. The student must submit the request to withdraw in writing to the Office of Student Services. A grade of W also can be assigned by the faculty or the Office of Student Services for administrative purposes. Students who drop a course after 25 percent of the course is completed will receive a grade of F, unless he or she can provide documented evidence of unusual and extenuating circumstances (e.g., serious illness, deployment to combat zone).

Capstone Grade Policy

The letter grade B is the lowest possible passing grade for Capstone. Students may retake the capstone only once. Students who are unsuccessful after their first Capstone attempt may be required to meet additional graduation requirements.

Grade Submission

Faculty will assign a grade for each student in accordance with the NDU grading policy. The faculty will submit course grades to the University Registrar via the appropriate electronic resources. A faculty member cannot change a student's grade after the course grade has been submitted. Any grade alteration request must provide documentation specifying the reason and have the approval of the Dean of Faculty and Academic Programs, and the University Provost.

Grade Appeal Policy

Students may appeal their grade on any assessment for which they feel the instructor has abused their discretion or issued an arbitrary or capricious grade. In every case, the burden of proof rests with the student to demonstrate a cause for a change in grade. The student has seven (7) workdays after receiving the grade and assessment feedback from the instructor to file a written appeal via memorandum with the Course Director

In the event that the Course Director is also the student's instructor, the student should deliver the Appeal memo to the college Associate Dean of Faculty. For a student taking an elective taught by a faculty member from a different college, the process is the same except the student would file their appeal with instructor's college Associate Dean. Similarly, for a student taking an NDU elective (one offered by non-college faculty), the student will file their appeal with the Deputy Provost.

Prior to initiating a grade appeal, the student should meet with their instructor to discuss their performance on the assessment. As a professional courtesy, the student should inform the instructor if they intend to file an appeal.

Upon receipt of the Appeal memo, the Course Director (or Associate Dean or Deputy Provost) will have 7 work-days to conduct an assessment and issue a ruling to the student. In all cases, the same timelines apply; 7 work-days to file an Appeal, and 7 work-days for final adjudication.

Academic Integrity

CIC has a zero-tolerance policy toward plagiarism and other breaches of academic integrity and will enforce the National Defense University Statement on Academic Integrity. Students should consult the NDU website for the most up-to-date information on Academic Integrity https://www.ndu.edu/Academics/Academic-Policies/.

Statement On Academic Integrity

NDU shall always foster and promote a culture of trust, honesty and ethical conduct. This statement on academic integrity supports the above guiding principle and applies to all components of the National Defense University. The purpose of this broad university policy is to establish a clear statement for zero tolerance for academic dishonesty and to promote consistent treatment of similar cases across the University on academic integrity and the integrity of the institution. This document should not be interpreted to limit the authority of the University President or the Vice President for Academic Affairs. This policy includes two key areas: academic integrity as it applies to students and participants at National Defense University; and academic integrity as it applies to assigned faculty and staff.

Breaches of Academic Integrity

Breaches of academic integrity include, but are not limited to:

- Falsification of professional and/or academic credentials.
- Obtaining or giving unauthorized aid on an examination.
- Having unauthorized prior knowledge of an examination.
- Doing work or assisting another student in their work without prior authorization.
- Unauthorized collaboration; multiple submissions.
- Plagiarism; and breaking the non-attribution policy.

Students are required to provide accurate and documentable information on their educational and professional background. Students admitted with false credentials are subject to university sanction.

Unauthorized collaboration is defined as students working together on an assignment for academic credit when such collaboration is not explicitly authorized in the syllabus or by the instructor.

Multiple submissions are instances in which students submit papers or other work that were or are currently being submitted for academic credit to other courses within NDU or at other institutions. Such work may not be submitted at NDU without prior written approval by both the NDU instructor and approval of the other institution.

Plagiarism is the unauthorized use of intellectual work of another person without providing proper credit to the author. All types of scholarly work, including but not limited to writing, computer code, speeches, slides, music, data and analysis, and electronic publications fall within these bounds. Plagiarism may be more explicitly defined as:

- Using another person's exact words without quotation marks and a footnote/endnote
- Paraphrasing another person's words without a footnote/endnote
- Using another person's ideas without giving credit via footnote or endnote
- Using information from the web without giving credit by means of footnote or endnote

To remind students of possible breaches of academic integrity, they are encouraged to submit their papers and assessments for review by plagiarism-detecting software prior to submission for grading.

Sanctions for Breaches of Academic Integrity

Sanctions for breaching academic integrity standards include, but are not limited to disenrollment, suspension, denial or revocation of degree, diploma, or certificate, a grade of no-credit with a transcript notation of "academic dishonesty", rejection of the work submitted for credit, letter or admonishment, or other administrative sanctions. Members of the United States military may be subject to non-judicial punishment or court-martial under the Uniform Code of Military Justice.

Academic Review Board

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

Students referred to the Academic Review Board will be notified via email. The communication will include a summary of the reason for the referral and request the student to appear before the Academic Review Board.

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

Remediation

Colleges will follow their own internal remediation policies except as noted below:
a. Any assessment, regardless of point or percentage value in a course, where a student earns a C (Unsatisfactory Performance) or lower will be remediated.

b. Under normal circumstances, the remediation will occur under the same conditions as the original assessment. For example, if the assessment is an in-class essay, the student will take another in-class essay; if it is an oral comprehensive exam, the student will take another oral comprehensive exam. Deans of Faculty are authorized to modify the conditions for the remedial assessment on a case-by-case basis.

c. To facilitate the most effective learning environment and not overwhelm the student with additional assessments, the reassessment will occur in a timely manner, usually no later than 7 calendar days after the remedial instruction is complete.

d. Upon successful remediation, the student will receive a grade no higher than a B- (80%) and the instructor will annotate the remediation process in the student's record.

Non-Attribution Policy

Presentations by guest speakers constitute an important part of CIC curriculum. In order that these guests, faculty, and other officials may speak candidly, the College guarantees that presentations and remarks will be held in strict confidence. Without the explicitly expressed permission of the speakers, nothing they say may be attributed to them directly or indirectly in the presence of anyone who was not authorized to attend the presentation. This policy is not intended to preclude references by students and faculty within the academic environment to opinions expressed by speakers. However, courtesy, good judgment, and the non-attribution policy preclude citing those views, even if the speaker is not identified by name. Specifically, the non-attribution policy provides that:

- Classified information gained during these presentations may be cited only in accordance with the rules applicable to its classification. Additionally, without consent, neither the speaker nor the College may be identified as the originator or source of the information.
- Unclassified information gained during lectures, briefings, and panels may be used freely within the academic environment; however, barring consent, neither the speaker nor the College may be identified as the originator of the information.
- Breaking the non-attribution policy is a breach of academic integrity.

Guest Speaker Procedures

Students are to be seated at least 5 minutes prior to the scheduled starting time and will stand when the guest speaker(s) enters the room. As a courtesy, students will not enter late or leave the room prior tothe conclusion of the event. It is customary to applaud the visiting speaker at the end of the introduction and to stand and applaud the visiting speaker at the end of the lecture and question-and-answer period.

Questions are essential to a productive discussion session with guest speakers. CIC expects students to be prepared and willing to ask high-quality questions of the speaker. When asking questions, students must identify themselves and state their parent institutions/bureau/agency/etc.

Speaker presentations and their associated question-and-answer sessions customarily are not recorded or transcribed, and never without the expressed consent of the speaker. This policy is complementary to the non-attribution policy.

Audio and Video Recording Policy

The College's policy on video/audio recording of lectures is subject to the consent of the speaker. CIC will respect the wishes of the speaker if consent to record presentations is withheld. All video/audio records are subject to disclosure to members of the public, pursuant to the Freedom of Information Act of 1974. All speakers are notified of this policy in writing in the letter of invitation. Each speaker is requested to sign a release prior to the lecture being recorded. Personal digital video or audio recording of Hopper Auditorium or Lincoln Hall is strictly forbidden.

Attendance Policy

Students are expected to participate in all scheduled class sessions and activities. The College will not issue course credit (or P for non-credit) if more than five percent of class is missed.

Absence from class activities degrades the continuity and effectiveness of the education process for all involved. Accordingly, absences may be authorized only under the most extenuating circumstances. Students are responsible for any missed coursework.

Course directors may approve a maximum of two hours of missed class time. All absences exceeding two hours must be pre-approved by the Dean of Students.

NDU Code of Conduct

To advance the mission of educating, developing, and inspiring national security leaders, we must continually create and maintain an academic environment founded in a community of trust that demands excellence in professional conduct and ethical standards. Students must adhere to the highest standards of honor. Specifically, students will not lie, cheat, steal, or otherwise behave in any way that discredits themselves or impugns the reputation of their fellow students at National Defense University. Failure to follow these standards may result in administrative action, including dismissal from the University.

Dress Policy

Military and civilian personnel are expected to exemplify professional standards of dress and appearance. A business suit with tie or conservative sport coat with tie is considered appropriate dress for men; commensurate attire is expected of women. Military students may wear either a class B uniform or civilian attire as described above. Some events will require military students to wear their Dress Uniform.

Spouse travel

NDU policy prohibits spouses and family members accompanying or meeting students and faculty members on field studies. This policy is strictly enforced and exists to eliminate any possible perceptions that field studies are not a full-time, professional endeavor.

Student Appeals

Student appeals are directed through the Office of the Dean of Faculty and Academic Programs for review and decision. Only written appeals with written documentation will be considered. Appeals should be submitted via email to CIC Dean@ndu.edu.

Student Services and Resources

NDU CIC Office of Student Services

The NDU CIC Office of Student Services (OSS) is in Room 145, Marshall Hall. Students should consult the OSS for assistance with admissions, registration, course management, tuition processing, and online student information system operations. Office hours are 0700-1500. The Office of Student Services can be reached by phone at (202)685-6300 and by email at CICOSS@ndu.edu.

Disability Support

The Americans with Disabilities Act (ADA) provides civil rights protection for persons with disabilities. This legislation guarantees a learning environment that provides for reasonable accommodation for students with disabilities. If you believe you have a disability requiring an accommodation, please contact the NDU CIC Office of Student Services.

Directions to Fort McNair

Ft. McNair Campus Fort Lesley J. McNair
300 5th Avenue
Washington, DC 20319

Enter via the Visitor's Gate (2nd St NW) for vehicle and foot traffic. DoD (military or civilian) or government photo ID required for entry. DC area and facility badges are not valid for entry.

Vehicles may be searched and are mandatory for some and random for all. If directed to report for a vehicle search, you must comply. All personal belongings brought into this post are subject to search.

Security

Students must present valid ID at the Marshall or Lincoln Hall Guard Desks upon entering the buildings, and visibly display ID badges in a visible place while participating in CIC courses. The Guard Desk can be reached at (202)685-3766. All personal property should always be secured. Do not leave purses or wallets in classrooms during breaks. Do not leave personal articles and clothing in the building overnight.

Class Hours

Resident classes start at 0800 and end by 1700 each day. Breaks are scheduled throughout the day. Hours for Distance Learning (DL) classes may vary. Consult course syllabus for details. Students are expected to be prompt and prepared for all courses.

Transportation

The DC area has several public transportation options. Information can be found at the following links:

- Washington, DC Metro: https://wmata.com/

- Virginia Railway Express: https://www.vre.org/
- Maryland MARC Train: https://www.mtamarylands.com/services/marc
- Amtrak Railway: https://www.amtrak.com/

Lost and Found

Report or turn in lost/found articles to the security guard on duty in the building where the article was lost/found. If theft of an item is suspected, first check to see if it has been turned in to the security guard. If not, notify the CIC Office of Student Services, the NDU Security Office, and the Fort McNair Military Police (MPs). After the MPs complete their report, the case is turned over to Fort Myer for investigation. When complete, a claim can be made against the government. Government claims require two estimates of loss with the Standard Form (SF) 95 when filing at the Fort Myer Claims Office: (703)696-0761. In general, the government will not pay a claim unless the stolen property was properly secured at the time of theft.

Inclement Weather

When adverse weather conditions in the Washington, DC area necessitate closing federal offices, the University will also close. Students should call (202) 685-4700 from an off-campus phone to obtain guidance. Press option #2 at the voice menu. Alternately, students can check the OPM website at: http://www.opm.gov/status. In the event that CIC is closed or has a two-hour delay, students should check with their instructors via Blackboard or email to determine whether alternate course plans will be implemented.

NDU Library

The NDU Library is a world-class academic library with a full complement of resources, services, and staff dedicated to ensuring all students achieve academic success. It is a 24/7 virtual library with branches in Washington, DC and Norfolk, VA. The Washington, DC library is in Marshall Hall.

Library Website – on campus: http://ndu.libguides.com/ndulib

Library Website – off campus: Use the "NDU Libraries" tab in Blackboard

MERLN: http://merln.ndu.edu

Hours: Monday-Thursday, 0700-1800; Friday 0700-1500 Location: 2nd and 3rd Floors, Marshall Hall

Telephone: 202-685-3511

Email: library_reference@ndu.edu

Services

Students all have access to ask-a-librarian, a virtual reference service that connects students to research assistance. Service to students emphasizes instruction on conducting independent research with the expert guidance of reference librarians, which allows students to explore the breadth of information on a topic and benefit from the discovery process. The library team teaches students to search effectively, evaluate information sources critically, synthesize selected sources into personal knowledge, and use information effectively in scholarship. Additionally, students have borrowing privileges to make use of the library's extensive collections of print, audio-visual, and electronic resources. On-campus students can attend a library orientation program that introduces them to a wealth of resources. A variety of additional research classes are offered in an online environment. Contact the library to inquire about current course offerings.

Collections

The library houses over 500,000 books, periodicals, and government documents covering a vast array of subject areas and topics. Blackboard accounts provide access to virtual collections including 100+ subscription databases covering an array of research topics, 20,000+ electronic journals, newspapers, dissertations, and magazines, and 125,000+ eBooks.

Special collections

Located on the upper level of the library, Special Collections, Archives, and History is the repository for personal papers, the NWC archives, student papers, lectures, rare books, and more. Exhibits which support the curriculum and special events, as well as artwork, are organized by Special Collections. A resource for the history of Fort McNair, the staff provides tours of the post and research support from local history collections.

Classified Documents Center

The library's Classified Documents Center is in Marshall Hall, Room 316. Proper clearance and positive identification are required to enter and use materials and services. Online networks (Intelink-TS and SIPRnet), secure meeting spaces, and storage boxes are available. Hours of operation are Monday-Thursday, 0730-1600; Friday, 0730- 1500.

MERLN

MERLN contains the most comprehensive collection of Defense White Papers and national security strategies available on the Web with contributions from more than 85 countries. MERLN features the Military Policy Awareness Links (MiPALs), custom-made research guides created by the library staff on topics such as Cybersecurity, National Security Strategy, Iraq, Iran, Afghanistan, and Terrorism. Each MiPAL offers U.S. policy statements supplemented by the latest collection of articles, reports, and analysis of U.S. policy options from a global network of think tanks. Additionally, MERLN hosts the U.S. National Strategy Documents, an in-depth collection that includes National Security Strategies dating from the Reagan Administration to the present day, Military and Defense Strategies, and Quadrennial Defense Review reports.

Campus Facilities

Subway

Subway is in Lincoln Hall and open Monday through Friday, 0700-1400, in Room 1501 near the passenger elevators on the first floor.

Fitness and Recreation Facilities

The main fitness center is located across from the NDU Lincoln Hall parking lot. Additional fitness centers are also located within the Roosevelt and Eisenhower Halls***.

***Currently closed for renovations.

Medical Assistance

Routine medical care for military personnel is available on post at the Fort McNair Health Clinic, Building 58, from 0630-1500; call (202) 685-3100 for an appointment. Military sick call is on a walk-in basis from 0630-0830 and 1130-1300. Physicals, immunizations, and other services can be obtained by appointment.

US Post Office

A USPS branch office is in Building 29 (202) 523-2144), just inside the ceremonial gate. Hours of operation are 0815-1300 and 1400-1615 Monday through Friday. The facility is closed on Saturdays, Sundays, and recognized holidays.

Chapel

The Fort McNair Chapel, Building 45, is available for religious services, ceremonies, and programs. Call the Chaplain's Office at (202) 685-2856 for further information.

Shoppette/Gas Station

The Fort McNair shoppette and Gas Station is open 7 days a week from 0800-1700. To contact the shoppette, please call (202)484-5823.

State Department Federal Credit Union

Members of the State Department Federal Credit Union may conduct their banking at the Fort McNair branch in Building 41. The credit union can be reached at (703)706-5127.

Barber/Beauty Shop

Fort McNair's Barbershop and Beauty Salon are in Building 41. Hours vary, for more information, please call (202)484-2354.

ATM

There is a State Department Federal Credit Union ATM located outside the cafeteria in Lincoln Hall.

Telephone Services

In the case of an emergency, incoming calls for students should be made to the Office of Student Services during regular business hours (0700-1500). The Office of Student Services can be reached at (202)685-6300 or DSN 325-6300. OSS will contact students in their classroom.

Dialing from University Phones

- To dial DSN, dial 94 then the DSN number.
- To dial a commercial number, dial 991 then the area code and number, as appropriate.
- To dial internally within NDU, please press 685 and then the extension.

Faculty and Administration

Leadership

Cassandra Lewis, Ph.D.
Chancellor

Stuart Archer
Dean of Administration

Linda Baughman, Ph.D.
Director of Institutional Research

Jonathan Beasley, COL
Assistant Professor
Dean of Students

Jim Chen, Ph.D.
Associate Dean of Academic Programs and Planning

Nakia Logan
Director of Student Services

Frank Marlo, Ph.D.
Dean of Faculty and Academic Programs

Donna Powers
Director of Academic Support

Department of Cyber Strategy and Infrastructure

Marwan Jamal, Ph.D.
Department Chair
Professor

Keith Caldwell, LTC
Military Faculty

James Churbuck
Associate Professor of Practice

Mark Duke
Associate Professor of Practice

Amy Hamilton, Ph.D.
DOE Chair

Linda Jantzen
Assistant Professor

Mike Love, Ph.D.
Associate Professor

Kenneth Miller, Col
Military Faculty

Frank Nuno
Assistant Professor

Robert Richardson IV
DISA Chair

Joanna Shore, Ph.D.
Professor

Mike Stamat, Ph.D.
Military Faculty

Melissa Thomas, Ph.D.
Professor

Nalonie Tyrrell, LTC
Military Faculty

J.D. Work
Associate Professor

Department of Information Strategy and Disruptive Technology

Dorothy Potter, Ph.D.
Department Chair
Professor of Practice

Elena Bailey
Assistant Professor

Michael Brody, J.D.
DHS Agency Chair

Abdullah Clark, MAJ
Military Faculty

Howard Clark, Ph.D.
Associate Professor

Andrew Gadbois,
CDR Military Faculty
Sea Service Chair

John Giuseppe, CDR
Assistant Professor
Military Faculty

Jill Goldenziel, Ph.D., J.D.
Professor

David Harvey
Professor of Practice

Richard Love, Ph.D.
Professor

Charles McLaughlin
Professor of Practice

Domenic Savini
Federal Accounting
Standards Advisory
Board Chair

Joseph Schafer, Ph.D.
Professor

Brian Shott
DOS Agency Chair

John Sullivan
Professor of Practice

Gwyneth Sutherlin, Ph.D.
Assistant Professor

Harry Wingo, J.D.
Assistant Professor

Andrew Whiskeyman
Associate Professor

Staff

Steve Beland
Technical Writer Ctr

Ishid Camp
Student Services Ctr

Deanna Fisher
Research Fellow

Kendra Ostrowski
Academic Specialist

Frederick Pack IV, Maj
Director of Operations

Scott Riess
Admin Support Ctr

Judy Robertson
Student Services Ctr

Noah Stevens III
Academic Support Ctr

Tamera Stringfield
Administrative Assistant Ctr