Academic Catalog

College of Information and Cyberspace

AY 2022-2023

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 2022-2023

The 2022-2023 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. Equality, 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 27 June 2022

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

I am thrilled to welcome all of you to another year at the National Defense University College of Information and Cyberspace (CIC). Academic Year 2022-2023 promises to be another year of growth at the College, continuing the significant progress we have made as an institution. We continue to grow our team of world-class faculty and staff, expand our course offerings, and cement ourselves as a thought leader in Information and Cyberspace. I couldn't be more excited for the road ahead.

CIC Faculty have continued to impress, innovate, and lead within their areas of expertise. Engagements with Congress, academic journals, think tanks, the National Security Agency, Office of the Secretary of Defense, and much more highlight the breadth and depth of the work that we do. Simultaneously, CIC faculty have continued to provide world-class educational programs, course design, and teaching. They personify the mission, vision, and goals of CIC.

We have also continued to grow our staff, who have handled an incredibly heavy burden with aplomb and deftness. As our faculty, course offerings, and event lineups have continued to grow, CIC staff have adapted and evolved, and continued to deliver at a high level. The Second Annual Grace Hopper Award, Holocaust Remembrance Event, and multiple graduation ceremonies are just a tiny fraction of the excellent events that were put on this year.

CIC was thrilled to once again welcome back multiple in-person activities and events which we have missed in previous years. In continuation of our long-standing tradition of fostering the next generation of leaders in Cyberspace and Information, CIC hosted 90 students from the National Student Leadership Conference for an all-day event on an intro to national security, war gaming, and CIC. We also welcomed multiple events from the University Consortium for Cybersecurity, in part with the Office of the Under Secretary of Defense for Research and Engineering, National Security Agency, and more.

Lastly, I would like to thank prospective students, continuing students, and graduates of CIC. Our student body never ceases to amaze me. The breadth of experience and accomplishment, both academic and professional, is immense. We are fortunate to receive such a diverse and exceptional student body, and I hope you will continue to be a part of our mission.

Your time here at CIC is a moment to take a step back and reflect, but also to prepare yourself to take further strides in championing the United States, its partners, and its allies. Our field demands agility and foresight, and your experiences here at CIC are essential in facing down the most pressing issues of our time. Together, we can achieve that goal, and I look forward to taking that journey with you.

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 and cyber policy, strategy, and campaign plan options that achieve national security objectives and joint warfighting.
- 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 is in the process of being renamed to Strategic Information and Cyberspace Studies

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

Core Courses 30 Credit Hours (CH)
Cyberlaw
Foundations of the Information Environment
Information Warfare Strategy
International Challenges in Cyberspace
National Security Strategy
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)
Cyberlaw
Foundations of the Information Environment
Information Warfare Strategy
International Challenges in Cyberspace
National Security Strategy
Strategic Competition in the Information Environment
Strategic Leader Foundational Course
Strategic Thinking and Communication
Warfighting and Disruptive Technologies
**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

The Chief Information Officer Leadership Development Program (CIO LDP, or LDP for short) 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 six courses. The leadership skills and abilities are put into practice and the learned knowledge is employed as students participate in a domestic field study. The

domestic field study examines how private and public sector organizations implement CIO competencies. CIO LDP students form a learning community that fosters multiple perspectives on a wide range of issues

Academic Year 2022-2023 Cohort

- FALL: 10 August – 18 November 2022
- SPRING: 18 January – 28 April 2023

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 two courses (6 CH) from certificates programs to the MS degree whether these courses are electives or core courses. Students may apply a maximum of two courses (6 CH)

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.
- Apply data-sharing practices across organizations and systems that fulfill 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).
- Assess the emerging technologies (and underlying data) for their ability to enhance data-driven decision-making for strategic effect.
- Identify, shape, and formulate data strategies that ensure ethical and legal data availability and transparency, supporting multi-agency and/or multi-national collaboration, including collaboration with industry.

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
Warfighting 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)
- Full time In-residence (Leadership Development Program (LDP), 14 weeks, Fall and Spring semester)

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.
- 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.
- Apply critical, strategic, ethical, and innovative thinking to lead in national security organizations.

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
Warfighting 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

- Apply cybersecurity principles to protect and defend in cyberspace and traditional physical domains (i.e., air, space, land, and sea).
- Assess the opportunities for collaboration in cyberspace between the public and private sectors.
- Develop strategies that provide cyber security, risk management, security incident management, continuity of operations, and disaster recovery to cyber infrastructure.
- Evaluate disruptive and emerging technologies for their potential to change the character of war.
- Apply critical, strategic, ethical, and innovative thinking to lead in the development and use of cybersecurity strategies, plans, policies, enabling technologies, and procedures in cyberspace.

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

- Integrate cyber workforce leadership, cyber security strategies, and the strategic employment of cyber resources into a framework for achieving national security goals.
- Evaluate U.S., Allied, and adversary cyberspace and information policies and authorities with respect to national and international cyber law.
- Evaluate disruptive and emerging technologies for their potential to change the character of war.
- Create strategies and policies to defend against and respond to emergent and future cyber threats.
- Apply critical, strategic, ethical, and innovative thinking to lead in national security organizations.

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
Warfighting and Disruptive Technologies

Information Technology Program Management Graduate Certificate

Modalities

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

Certificate Learning Outcomes

- Apply program management skills to lead and manage complex IT acquisition and other projects and programs that create value for their organizations 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.
- Assess 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.
- Apply principles of strategic leadership to include effective communication, creative and critical thinking, decisions making, and ethical conduct.

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.

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 assets.

Cyber Intelligence 6232 (CYI)

This course examines the cyber leader's role in cyberspace intelligence. As decision makers, cyber leaders both enable and consume intelligence related to cyberspace, both formulating and implementing intelligence policy and strategy, and planning and executing intelligence activities in cyberspace. The course includes perspectives and issues applicable to

the U.S. Intelligence Community (IC) in general and elements unique to cyberspace. It is not intended to impart intelligence-specific skills and tradecraft to professional intelligence officers, and no prior experience in or knowledge of intelligence is required.

Cyberlaw 6204 (CBL)

The Cyber Law course presents an overview of the structure of the US domestic and international legal systems. It introduces students to the philosophical foundation of the legal system and the sources of domestic and international law. During the course, students will be taught the process of legal reasoning and how the process is broadly applicable in professional writing and speaking, and will be given the opportunity to practice the skills they learn. Among other things, the course will discuss the role of attorneys in national security and international law; how senior leaders interact with attorneys and their advice; and the use of legal reasoning in the development of policy and strategy. Throughout the course, the relevance of all the topics discussed to cyberspace, cyber operations, and information as an instrument of national power is paramount.

Cyber Security for Information Leaders 6021 (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.

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 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.

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

Risk Management for Senior Leaders 6218 (RML)

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 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.

Strategic Leadership Foundational Course NDU6000 (SLFC)

This course provides 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 cyberspace fundamentals and information theory and strategic principles.

White House, Congress, and Budget 6606 (WCB)

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.

2CH Elective Course Descriptions

These two credit hour courses are offered by CIC to all NDU MS resident students. CIC MS resident students may also select NDU electives offered by other NDU colleges (not described here).

Artificial Intelligence and National Security 6033 (AIN)

This elective focuses on the national security implications of innovation enabled by artificial intelligence. Participants review US national strategic opportunities and threats, AI's evolution into the domains of warfighting, and the AI activities of partners and competitors. Topics include machine learning, bias, big data, and autonomous systems, all within the context of military strategy and operations. The course provides students with the background and vocabulary to understand the role of AI capabilities at the strategic level. This is a course in the Data and Disruptive Technologies (DDT) elective concentration. **Big Data for Decision 6004 (BDD)**

This course explores the concepts of data management and data lifecycle as key components for improving mission

effectiveness through the development of enterprise wide and local data management strategies and programs. It examines management issues such as data governance and organizational information behaviors and values. The course uses the data lifecycle framework to introduce the concepts of 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.

Budgeting for National Security 6015 (BNS)

This course provides students with a comprehensive understanding of budget issues related to national security. The overarching goal is for students to develop leadership strategies to help shape their military, intelligence, and international agencies' fiscal environment, goals, and outcomes. The course focuses on topics such as the current budget environment, strategic performance and budget management, budget formulation, enactment, and execution. The course also examines leadership strategies for resource prioritization and decision-making, and managing relationships with executive and legislative branch oversight, command leadership and external organizations.

Cyber Security Awareness 6024 (CSA)

This elective explores concepts and practices of defending the modern net-centric computer and communications environment. The course covers the 10 domains of the Certified Information System Security Professional (CISSP®) Common Body of Knowledge (CBK®). In addition, the course covers a wide range of technical issues and current topics including basics of network security, threats, vulnerabilities, and risks, network vulnerability assessment, firewalls and intrusion detection, transmission security and TEMPEST, operating system security, etc.

Cyber Security in the 21st Century 6017 (CSL)

This elective 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 assets.

Cyberwarfare 6021 (CWF)

This course examines the use of cyber capabilities, including cyber-enabled information operations, in warfare, as well as outside the traditional bounds of armed conflict in support of national security interests. It will provide the technical, legal, and policy background necessary for the discussion. Different approaches to cyberwarfare are illustrated through lessons focused on the cyber activities of Russia, China, and Iran. Topics discussed include cyber espionage, theft of intellectual property, cyber-enabled influence operations, big data analytics, international humanitarian law, and international cyber norms.

Data Analytics for Decision Makers 6037 (DAD)

This elective provides an overview of data analytics with a focus on some of the key challenges and benefits in working with data on different scales. Students will analyze and evaluate qualitative and quantitative data sets to better enable senior leaders to meet mission needs and business priorities. Students will explore the application domain and the big picture of a complex system to track how data moves around among the relevant systems and stakeholders.

Frameworks for Enterprise Risk Management and Internal Controls 6013 (FRI)

This course examines how military and senior government leaders can enhance efficiency, effectiveness, accountability, and transparency with a focus on the areas of greatest risk within the national security environment. The primary focus is on the process of identifying potential risks and the actions necessary to reduce or eliminate their financial, programmatic, and operational impact and the achievement of efficient and effective operations, accurate and timely reporting, and compliance with laws and regulations.

Future Emerging Technologies 6030 (EIT)

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 analyze how emerging technologies evolve. They evaluate the international, political, social, economic, and cultural impacts of emerging technologies using qualitative and quantitative evaluation methods. Students assess emerging technologies using forecasting methodologies such as monitoring and expert opinion, examining future trends, and assessing international perspectives.

Illicit Activities in Cyberspace 6026 (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 ranges from illicit actors and their use of cyberspace to the government, law enforcement, and industry ability and authority to respond to illicit activities in cyberspace

Influence Warfare 6047 (IWF)

Never fight fair. And be ready to have your world turned upside down. This case-study-based strategy course is for every national security professional—actionable, practical, intrepid. Influence is central (but rarely studied as a cogent academic discipline) to both warfare and great power competition. Allows leaders to do more with less, with the tools they already have immediately at hand—to collapse adversaries silently and invisibly, outside traditional instruments of national power. Tools of influence include subversion, deception, sabotage, fifth columns, propaganda, disinformation, kompromat, glasnost, sisu, active measures, szalámitaktika, trust warfare, etc. Case studies range from CCP to the Kremlin, Finland to Taiwan, Estonia to Philippines, Tehran to ISIS in Africa, Facebook to Chevron, Purdue Pharma to Antifa, Boko Haram to Neo-Nazis, Marxists to anarchists, Huns to the

Mongols, Comanche to the Mayans, election interference to social media manipulation, and so much more. Short, thrilling, current readings/videos/podcasts. Lively in-seminar debates and wargames.

Protecting Critical Infrastructure against Cyber Attack 6018 (PCI)

This course provides a comprehensive overview of information assurance and critical information infrastructure protection. Information assurance of information assets and protection of the information component of critical national infrastructures essential to national security are explored. The focus is at the public policy and strategic management level, providing a foundation for analyzing the information security component of information systems and critical infrastructures. Laws, national strategies and public policies, and strengths and weaknesses of various approaches are examined for assuring the confidentiality, integrity, and availability of critical information assets. Learning Outcomes: Students will be able to analyze laws, national strategies, and public policies; and assess the strengths and weaknesses of various approaches for assuring the confidentiality, integrity, and availability of those information assets created, stored, processed, and communicated by information systems and critical information infrastructures.

Securing Cyberspace Through the Whole of Government 6010 (SCG)

This elective provides students of national security strategy with an understanding of the vital role played by the Federal, civilian interagency in achieving national cybersecurity objectives. This course will therefore examine Federal interagency cybersecurity strategies, policies, authorities, resources, capabilities, leading issues and challenges, through a series of case studies, point papers, and exercises so as to: (1) Analyze the objectives, authorities, and capabilities which define the Federal inter-agency's place and role in national cybersecurity strategy and risk management; (2) Evaluate the leading issues and challenges which shape Federal inter-agency strategies, policies and responses to priority, national cybersecurity risks, threats and vulnerabilities; and (3) Assess opportunities for and limitations of cooperation, collaboration and joint operations between the DOD, NSA and the Federal, civilian interagency towards common national cybersecurity strategic ends.

Subversion, Subterfuge, Sabotage 6046 (SSS)

Never fight fair. And be ready to have your world turned upside down (even if you were in the fall elective). This case-study-based strategy course is for every national security professional—actional, practical, intrepid. Subversion is central (but rarely studied as a cogent academic discipline) to both warfare and great power competition. Allows leaders to do more with less, with the tools they already have immediately at hand—to collapse adversaries silently and invisibly, outside traditional instruments of national power. This course differs from fall's "Influence Warfare" elective in that it focuses more surgically on subversion, subterfuge (a continuing effort to subversion), and institutional sabotage (an especially pernicious and effective form of subversion) of adversaries and competitors. And how to develop actionable, practical, intrepid strategies to collapse adversaries from the inside and protect national interests. New students along with graduates of fall's

"Influence Warfare" elective will equally find value in fresh new case studies and enhanced tradecraft. Tools of subversion include unrestricted political warfare, fifth columns, propaganda, third options, deception warfare, kompromat, glasnost, sisu, szalámitaktika, etc. Case studies range from the power of film to conspiracy theories, slave revolts/liberation to indigenous-rights movements, CCP to the Kremlin, Tehran to Muslim Brotherhood, far left/far-right extremists to separatist movements, OSS to modern urban guerrilla saboteurs, Marxists to anarchists, Attila the Hun to Genghis Kahn, Comanche to the Mayans, elections to social media trends, and so much more. Short, thrilling, current readings/videos/podcasts. Lively in-seminar debates and

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)

Academic Collaboration

In addition to the academic partners that accept CIC graduate credit, there are an array of educational and academic institutions that collaborate with our school and its people on a regular basis. Some of our team members, and the institutions they lead interactions with, include Gary Brown and the Massachusetts Institute of Technology (MIT) through the Roundtable on Military Cyber Stability (RMCS), Jonathan Henick and the Foreign Service Institute (FSI), Dr. Gwyneth Sutherlin and the North Atlantic Treaty Organization (NATO) Strategic Communications Center of Excellence, Harry Wingo and the US

Naval Academy (USNA), Joe Billingsley and the Institute of World Politics (IWP), and Michael Brody and the Center for Homeland Defense and Security at the Naval Postgraduate School (NPS).

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. Jim Chen of the CIC Cyber Strategy and Infrastructure Department.

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 Masters and CIO LDP:

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 2023 Semester: September 1, 2022
Summer 2023 Semester: February 1, 2023
Fall 2023 Semester: June 1, 2023

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 point values used for grading. B+ is the grade associated with median student performance. Quality points are used to calculate GPA, whereas point values are used for final course grades. Course letter grades and overall GPA are displayed on the student's transcript.

Letter Grade	Qualitative Descriptor	Quality Points	Point Value 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
F (For Pass-Fail designated course)	Fail	0.00	*	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 of 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

A student may appeal a final course grade if the student reasonably believes that they were graded in an arbitrary or capricious manner, and the student is unable to resolve his or her concerns with the faculty member who assigned the grade. This policy applies only to final course grades.

A student may only challenge a final course grade under the following conditions:

- The student has discussed their concerns with the faculty member who awarded the grade
- The student has evidence that the grade was awarded in an arbitrary or capricious manner

For the purposes of this policy, arbitrary or capricious means the assignment of a final course grade was made on a basis other than the student's academic performance in the course, and/or the assignment of a final course grade was made in a manner that substantially or unreasonably departed from the instructor's articulated standards.

This policy will not be used to review the judgment of an instructor in assessing the quality of a student's work, to require another faculty member to re-grade or re-examine a student's work, or in cases involving alleged violations of academic integrity.

Grade Appeal Process

1. If, after discussion with the faculty member, the student believes that the grade is arbitrary or capricious, or if there is an inability to reach the faculty member, the student may challenge the grade by sending a letter to the department chair no later than 30 calendar days after the grade has been posted. This letter must:
    a. Identify the course, date, and faculty member that awarded the grade;
    b. State the basis of the challenge, including all facts relevant to the challenge and the reasons the student believes the grade is arbitrary or capricious;
    c. Indicate the date(s) the student consulted with the faculty member regarding his or her concern(s) and summarize the outcome of those discussions; and
    d. Attach any supporting documentation the student believes should be considered in the challenge, including the course syllabus.

2. Upon receiving a written challenge of a final course grade, the Department Chair shall forward a copy of the challenge to the faculty member who assigned the grade.

3. The Chair will review the submissions and, if necessary, investigate to determine if the grade was arbitrary or capricious based on the definition outlined in this policy. A written decision will be issued to both parties within 15 calendar days.

4. Both parties have a right to appeal the Chair's decision by filing a written appeal within 10 business days to the NDU CIC Dean of Faculty and Academic Programs (The Dean). The written appeal should state the basis for the appeal and attach all relevant written documentation.

5. The Dean shall forward the appeal to the NDU CIC Academic Policy Committee. The Academic Policy Committee will review the submissions and may, at the Committee's discretion decide to hear statements from the parties. Following deliberations, the Committee will issue a recommendation to the Dean (or designee) indicating:

    a. Whether the Committee finds the grade to be arbitrary or capricious and;
    b. The Committee's recommendations for the disposition of the appeal.

6. The Dean (or designee) will review the Committee's recommendation and render a final decision in writing to the student, the faculty member, and the chair within 10 calendar days of receipt of the Committee's recommendation. The Dean's decision shall be final without further appeal.

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.

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 to

the 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

Food Service Operations

NDU's cafeteria is in Lincoln Hall. The Lincoln Hall Café*** is open Monday through Friday, 0700-1430, in Room 1501 near the passenger elevators on the first floor. For more information, call the cafeteria directly at (202) 685- 7235.

***COVID protocols have affected food service options on campus. For the most up-to-date news on food options please contact NDU Operations at NDU-Operations@ndu.edu.

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

Linda Baughman
Director of Institutional Research

Jonathan Beasley, COL
Assistant Professor
Dean of Students

Joe Billingsley
Director of Strategic Engagement

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

Nakia Logan
Director of Student Services

Donna Powers
Director of Operations

Russell Quirici
Dean of Administration

Department of Cyber Strategy and Infrastructure

Roxanne Everetts, DM
Department Chair
Professor

Perry Alexander, Lt. Col.
Military Faculty

Keith Caldwell, LTC
Military Faculty

James Churbuck
Associate Professor of Practice

Mark Duke
Associate Professor of Practice

Andrew Gravatt
Professor of Practice

Walker Hofmann, Lt Col
Military Faculty

Marwan Jamal, Ph.D.
Professor

Linda Jantzen
Assistant Professor

Kenneth Miller, Col
Military Faculty

Frank Nuno
Assistant Professor

Robert Richardson IV
Assistant Professor
Defense Information Systems Agency Chair

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

Howard Clark, Ph.D.
Associate Professor

Andrew Gadbois, CDR
Military Faculty
Sea Service Chair

John Giuseppe, CDR
Assistant Professor
Military Faculty

David Harvey
Professor

Brent Kauffman, LTC
Military Faculty
Army Chair

Richard Love, Ph.D.
Professor

John O'Brien
Associate Professor of Practice

Joseph Schafer, Ph.D.
Professor

Gwyneth Sutherlin, Ph.D.
Assistant Professor

Harry Wingo, J.D.
Assistant Professor

Brian Shott
DOS Agency Chair

David Thaw, Ph.D.
Professor

John Sullivan
Professor of Practice

Andrew Whiskeyman
Professor

Adjunct Faculty

Catherine Downes, Ph.D.
Professor

Veronica Wendt, Ph.D.
Candidate
Grant Support

Domenic Savini
Federal Accounting Standards Advisory Board
Chair

Staff

Aaron Adams
Academic Support/Operations

Michaela Ibrahim
Instructional Designer

Jacob Sharpe
Research Analyst

Steve Beland
Technical Writer Ctr

Ray Ivy
Logistics Support Ctr

Mekhi Simmons
Academic Support Ctr

Ishid Camp
Student Services Ctr

Kendra Ostrowski
Academic Specialist

Tamera Stringfield
Administrative Assistant Ctr

Lauren Dixon
Student Support Ctr

Frederick Pack IV, Capt
Military Staff

Deanna Fisher
Research Fellow

Scott Riess
Admin Support Ctr

Ryan Hammond
Administrative Assistant Ctr

Judy Robertson
Student Services Ctr