



## CHIEF INFORMATION OFFICER



The National Defense University (NDU) College of Information and Cyberspace (CIC) Chief Information Officer (CIO) Program is the recognized leader in graduate education for Federal CIO leaders and agency personnel. It directly aligns with the Federal CIO Council-defined CIO competencies and addresses the Clinger-Cohen Act and other relevant legislation mandates as well as the current administration's interpretations and implementations of these legislative actions.

CIO Program graduates earn a certificate signed by the DOD CIO and the NDU CIC Chancellor that recognizes they have earned an education in the Federal CIO competencies. The CIO Certificate Program is organized around subject areas directly related to CIO competencies identified by the Federal CIO Council. Selected courses allow students to tailor their CIO program of study to meet their organization's needs and priorities. Additionally, the CIO Certificate is a concentration in the Government Information Leadership (GIL) Master of Science Degree.

### *Successful CIO graduates will be able to:*

- 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.

### GIL Master of Science Degree CIO Concentration

The 36 credit curriculum of the Government Information Leader Degree offers a combination of information management, technology, and leadership intensive courses in a collaborative and interactive environment. Students earn the Master of Science degree by successfully Students may apply up to 15 graduate-level credit hours completing twelve (12) courses.

**7**

Required  
Courses

**3**

Leadership/  
Management Courses

**1**

Technology  
Course

**1**

Security  
Course

### Minimum Admissions Eligibility Criteria:

- Bachelor's degree (3.0 GPA minimum)
- Civil service pay grade of GS-13 or Officer Rank of O-4

For more information refer to the CIC website or catalog.

## GIL Master of Science Degree

### CIO Concentration Requirements (12 Courses)

<b>Foundational (3)</b>	<i>NSC</i> (6329)	National Security and Cyber Power Strategy
	<i>OCL</i> (6321)	Organizational Culture for Strategic Leaders
	<i>CAP</i> (6700)	Capstone
<b>Core (4)</b>	<i>CIO</i> (6303)	CIO2.0 Roles and Responsibilities
	<i>ITA</i> (6415)	Strategic Information Technology Acquisition
	<i>PFM</i> (6315)	Capital Planning and Portfolio Management
	<i>SPB</i> (6328)	Strategic Performance and Budget Management
<b>Leadership/Management (Take 3)</b>	<i>ARC</i> (6412)	Enterprise Architectures for Leaders
	<i>DMG</i> (6323)	Decision Making for Government Leaders
	<i>IPL</i> (6411)	Information Technology Program Leadership
	<i>ITP</i> (6416)	Information Technology Project Management
	<i>LDC</i> (6301)	Leadership for the Information Age
	<i>MAC</i> (6512)	Multi-Agency Information-Enabled Collaboration
	<i>PRI</i> (6333)	Strategies for Process Improvement
<b>Technology (Take 1)</b>	<i>SLP</i> (6318)	Strategic Leader Theory and Practice
	<i>DMS</i> (6414)	Data Management Strategies and Technologies
	<i>EIT</i> (6442)	Emerging Technologies
	<i>GEN</i> (6205)	Global Enterprise Networking and Telecommunications
<b>Security (Take 1)</b>	<i>WGV</i> (6435)	Web- Enabled Government: Facilitating Collaboration and Transparency
	<i>AII</i> (6203)	Information Assurance and Critical Infrastructure Protection
	<i>COO</i> (6504)	Continuity of Operations
	<i>ESS</i> (6206)	Enterprise Information Security and Risk Management
	<i>SAC</i> (6444)	Strategies for Assuring Cyber Supply Chain Security
	<i>SEC</i> (6201)	Cyber Security for Information Leaders
	<i>TCC</i> (6215)	Terrorism and Crime in Cyberspace

