

**CLEARED
For Open Publication**

Dec 09, 2022

Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW



DOD CHIEF INFORMATION OFFICER (CIO)

Department of Defense Cyber
Scholarship Program: 2022 – 2023
Retention Program Guidelines

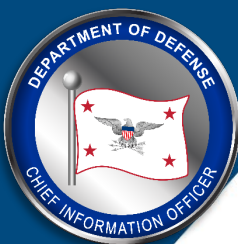


Table of Contents

Program Details.....	3
Program Definitions	3
Eligibility Requirements	3
Scholarship Quotas.....	4
Program Costs.....	4
Available Degree Programs/Paths and Academic Start Dates.....	5
PhD.....	5
Master’s.....	5
Graduate Certificates.....	6
Associate’s.....	6
Other Programs	6
Obligations.....	6
Continued Service Agreement Requirements.....	7
Notification of Acceptance—All Schools	7
Retention Program Applicant Process.....	8
Application Requirements.	8
For all Graduate Programs (Master’s, PhD, certificate) or JCAC:.....	8
For Associate Degree Programs:.....	9
Retention Program Component Office of Primary Responsibility Process.....	10
Programs	11
Air Force Institute of Technology (AFIT)	11
Naval Postgraduate School (NPS).....	13
Joint Cyber Analytics Course (JCAC).....	18
DoD CySP Community College Program	19

Program Details

This document provides details on the academic opportunities offered under the Department of Defense Cyber Scholarship Program (DoD CySP) Retention Program. After reading this document in its entirety, DoD Agencies/Components/Military Departments (hereinafter referred to as Components) and scholarship applicants can use the DoD CySP Retention Application and apply from May 23, 2022 – June 30, 2022 at: <https://www.dodemergingtech.com/cyber-scholarship-program-cysp/>.

The DoD CySP is authorized by Chapter 112 of title 10, United States Code, Section 2200. The purpose of the program is to support the recruitment of new cyber talent and the retention of current highly skilled professionals within the DoD cyber workforce. Additionally, this program serves to enhance the national pipeline for the development of cyber personnel by providing grants to higher education institutions. The DoD CySP is sponsored by the DoD Chief Information Office and administered by the National Security Agency (NSA). The overall program timeline for 2022 – 2023 is detailed in Table 1: CySP Retention Program Timeline.

Table 1: 2022 – 2023 CySP Retention Program Timeline

Description	Timeline
Application window	May 23 – June 30, 2022
Component nomination review	July 1 – 8, 2022
CySP Program Office review	July 8 – 15, 2022
Applicants notified of status	July 18, 2022

Program Definitions

- **Components:** Any DoD Agency, Organization, or Command.
- **Component Office of Primary Responsibility (OPR):** Office within the Component that will represent that component to the DoD CySP Program Office. The OPR will advertise the program within the Component.
- **Applicant:** DoD civilian or active-duty military member.
- **Application Package:** Completed package submitted electronically in the DoD CySP Retention Application.
- **Nomination Statement:** Completed by the OPR in the DoD CySP Retention Application.

Eligibility Requirements

The DoD CySP program is open to U.S. citizens who meet the following requirements:

- Active-duty military members (currently not performing a period of obligation service for another program).

- Traditional Reservist and National Guard members who are in an active-duty status may apply as long as they are eligible to attend an education program while on active-duty.
- Permanent DoD civilian employees who have completed any required probationary time.
 - Temporary, conditional, or employees on performance improvement plans are not eligible to apply for the DoD CySP.
 - Currently not performing a period of obligated service for any programs.
- Nominated by their Component.
 - Components shall only nominate employees who are high performing military members/civilians rated at the upper (e.g., above satisfactory) levels of the applicable performance appraisal system and who demonstrate sustained quality performance with the potential of increased responsibilities.
 - Components shall also confirm that participating in an education program will not negatively affect any service or job duty requirements (e.g., Rated Officers, special pay band/Military Occupational Specialty code/Occupational Series).
- Meet all requirements for acceptance to the specific institution they plan to attend.
 - All eligibility criteria, especially academic credentials, should be carefully reviewed as DoD CySP requirements may be more stringent than general academic enrollment criteria for a particular academic institution. No waivers will be granted.

Scholarship Quotas

No quotas have been identified. The actual number of scholarships available will be contingent on the total number of eligible applicants and available funding. Component OPRs are responsible for administering the nomination process for their organization. The Component OPR shall ensure all applicants fulfill the specific academic and personnel development requirements (e.g., individual development plans). The Component OPR is responsible for submitting the nomination statement within the DoD CySP Retention Application. The nomination statement may prioritize the applicants in order of the Component's priorities. Components should prioritize applicants separately for the available degree programs/paths as identified within the nomination statement.

Program Costs

Cost of tuition, required fees, and required books (any recommended books or materials are not covered) will be covered by the DoD CySP. Selected applicants will continue to receive their military pay or civilian salary from the Component throughout their course of study. Component OPRs are responsible for any PCS costs associated with the degree program. For example, Components are responsible for travel/permanent change of station (PCS) costs to and from the academic institution and any necessary position back-fill for selected applicants. The DoD CySP will fund any short-term, degree specific on-campus activities (e.g., cohort requirements, short-term TDYs). Academic institutions will identify any degree specific on-campus activities that require travel. It is highly recommended that prospective applicants meet with their Component OPR to discuss all program costs. This meeting

should provide a full understanding of what is expected during their education experience and upon completion of the academic degree.

The DoD CySP is funded annually. All participation is contingent upon available funding.

Available Degree Programs/Paths and Academic Start Dates

The following list of degree programs/paths are the only options through the DoD CySP Retention Program. The DoD CySP Retention Program does not offer scholarships to attend a school of choice or to pay for degree programs currently in progress. The DoD CySP will not pay for “like” degrees. Individuals who already hold a degree in Cyber, Information Technology, Information Assurance, Computer Science, or any other related technical field may apply, but for the next level higher. *Example: An applicant who currently has a Master’s in Computer Science would be eligible to apply for a PhD/Doctorate Program, but not another Master’s Program.* Additional information on the programs listed below can be found in follow-on sections of this document.

PhD

- **Air Force Institute of Technology:** *(Full-time / In-Resident ONLY) (January 2023 or August 2023)*
 - PhD in Computer Science
 - PhD in Electrical Engineering
 - PhD in Computer Engineering
- **Naval Postgraduate School:** *(Full-time / In-Resident ONLY) (January 2023 or July 2023)*
 - PhD in Computer Science
 - PhD in Electrical and Computer Engineering
 - PhD in Information Sciences
 - PhD in Mathematics

Master’s

- **Air Force Institute of Technology:** *(Full-time / In-Resident ONLY) (January 2023 or August 2023)*
 - Master of Science in Cyber Operations
 - Master of Science in Electrical Engineering
 - Master of Science in Computer Engineering
 - Master of Science in Computer Science
 - Master of Science in System Engineering (Cyber Systems)
- **Naval Postgraduate School:** *(Full-time / In-Resident ONLY) (January 2023 or July 2023)*
 - Master of Science in Computer Science
 - Master of Science in Cyber Systems and Operations
 - Master of Applied Cyber Operations
 - Master of Science in Electrical Engineering / Engineering Science

- *Master of Business Administration in Information Systems Management*
- *Professional Master's of Business Administration*
- *Professional Master's of Business Administration (Part-time / Distributed Learning¹)*

Graduate Certificates

- *Naval Postgraduate School (Possible for Part-time / Distributed Learning) (January 2023 or July 2023)*
 - See NPS information on page 11 for additional guidance.

Associate's

- *Eastern New Mexico University – Ruidoso Branch (Both Full-time / Part-time & In-residence / Distance Learning) (January 2023 or August or September 2023)*
 - Associate of Science – Information System Cybersecurity

Other Programs

- *Joint Cyber Analysis Course (JCAC) Partner Program (Active-Duty Military ONLY) (August or September 2023)*
 - JCAC is housed at the Information Warfare Training Command Corry Station, Pensacola, Florida.
 - Utilizing pre-established NSA agreements, graduates of the JCAC program may transfer credits into an undergraduate or graduate program.
 - DoD CySP Program Office cannot assist interested military service members with acceptance to the JCAC Program.

Obligations

All applicants will be required to sign a continued service agreement (CSA). Retention students shall fulfill post-academic service obligations pursuant to 10 U.S.C. 2200a. Program participants are obligated to maintain good standing in their degree programs, to continue as a program participant. If a program participant does not maintain a good standing in their degree program, they will be responsible for **repaying the program costs for failure to complete the degree program satisfactorily and/or to fulfill the service commitment consistent with 10 U.S.C. 2200a(b)(2) and (3) and the policies of the Department and the respective Component.** All required documents and agreements will be captured in the DoD CySP Retention Application.

¹ Distributed learning is synonymous with distance learning

Continued Service Agreement Requirements

- Members of the Military Services shall serve on active duty while fulfilling service obligations defined by their respective Component. While the service obligation is at the discretion of the respective Component, members of the military services may use the following times as a baseline:
 - 2 years for the Community College program.
 - 4 years for an undergraduate program (JCAC – only).
 - 3-5 years for graduate programs (Graduate Certificate, Master’s, PhD, and Doctorate).
- DoD civilian employees shall sign a CSA with their parent organization or Component that complies with 10 U.S.C. 2200a, prior to commencement of their education, to continue service within the DoD upon conclusion of their education, for a period equal to:
 - 3 years for the Community College program.
 - 5 years for graduate programs (Graduate Certificate, Master’s, PhD, and Doctorate).
 - NOTE: The Component OPR may put additional service requirements on the applicant.

If selected, applicants may be required to additionally sign a Student Code of Conduct Agreement, a Family Educational Rights and Privacy Act (FERPA) waiver required for release of transcripts, and other additional forms as required.

Notification of Acceptance—All Schools

Based on funding, a determination on the number of DoD CySP scholarships to be awarded will be made by the DoD CySP Scholarship Program Steering Committee. The DoD CySP Program Office will formally notify the OPRs and students about applicant acceptances by **July 18, 2022**.

Retention Program Applicant Process

All applicants are responsible for submitting an unclassified application through the DoD CySP Retention Application.

Each package must include all items listed below.

Please redact any personally identifiable information (PII).

Incomplete applications will be rejected, with no exceptions. Applicants should take the time to go over their application with their management chain and/or Component OPR to ensure the package is complete. Applicants must utilize the DoD CySP Retention Application and submit applications by June 30, 2022.

Application Requirements.

For all Graduate Programs (Master's, PhD, certificate) or JCAC:

- Applicant's contact information
 - Agency
 - Agency mailing address (include office designator or command name)
 - Government email address
 - Phone numbers (voice/fax)
- Supervisor contact information
 - Name and Title
 - Email address
 - Phone numbers (voice/fax)
- Next Level Supervisor contact information
 - Name and Title
 - Email address
 - Phone numbers (voice/fax)
- Component OPR contact information
 - Name
 - Email address
 - Phone numbers (voice/fax)
- List of previous colleges/universities attended
 - School name and years attended
 - **Conferred Degree,² if applicable**, Program of Study
 - Grade Point Average (GPA) – Note: The DoD CySP requires that all applicants pursuing a master's degree must have an appropriate bachelor's degree with a minimum 3.0 GPA. Additionally, applicants pursuing a PhD/Doctorate must have an appropriate master's degree and a minimum 3.2 GPA.
 - Proposed college/university (AFIT, NPS, JCAC Partner Program). Applicants may provide up to three choices, placed in order of priority. The following must be included for each proposed college/university:
 - Proposed degree program

² Students applying for a master's program must have a conferred undergraduate degree and students applying for a PhD program must have a conferred graduate degree.

- Proposed start date
- Proposed student status
 - All students attending AFIT or NPS for a Master's or PhD are full-time
 - All students attending NPS for a Certificate Program may be full-time or Part-time
 - JCAC Partner Program applicants must include requested Partner University - full-time or part-time
- Additional required documents: (PII should be redacted)
 - Military or civilian personnel resume.
 - Most recent SF-50 – Notification of Personnel Actions (Applies to DoD civilians only).
 - Applicant's personal goals statement.
 - Signed CSA.
 - Recommendation from the applicant's supervisor. **The recommendation should highlight how the student's cybersecurity education will be applied by the Component following graduation.**
 - Endorsement from the applicant's second- or next-level supervisor. Please note that this endorsement and the recommendation from the first-level supervisor (noted above) are two separate documents. **The endorsement should highlight how the student's cybersecurity education will be applied by the Component following graduation.**
 - Copies of GRE or GMAT scores for nominees pursuing a **graduate level program**. (This is a DoD CySP requirement for all *graduate level programs*.) AFIT, NPS, and JCAC Partner Universities each have their own minimum GRE/GMAT score requirements. Applicants are responsible for ensuring they research and meet the minimum GRE/GMAT requirement for their Partner University of choice (if applicable).
 - Transcripts – Official or unofficial
 - If unofficial transcripts are provided and the student is selected to receive a scholarship, the DoD CySP Program Office may request official transcripts.

For Associate Degree Programs:

- Applicant's contact information
 - Agency
 - Agency mailing address (include office designator or command name)
 - Government email address
 - Phone numbers (voice/fax)
- Supervisor contact information
 - Name and Title
 - Email address
 - Phone numbers (voice/fax)
- Next Level Supervisor contact information
 - Name and Title

- Email address
 - Phone numbers (voice/fax)
 - Component OPR contact information
 - Name
 - Email address
 - Phone numbers (voice/fax)
 - Proposed Community College. Applicants may provide up to three choices, placed in order of priority, or leave this section blank. The DoD CySP Program Office will work with the applicant to identify institutions who have agreed to participate in the program. If applicants do provide up to three choices, the following must be included for each proposed college/university:
 - Proposed degree program
 - Proposed start date
 - Proposed student status
 - Full-time
 - Part-time
- Additional required documents: (PII should be redacted)
 - Military or civilian personnel resume.
 - Most recent SF-50 – Notification of Personnel Actions (Applies to DoD civilians only).
 - Applicant’s personal goals statement.
 - Signed CSA.
 - Recommendation from the applicant’s supervisor. **The recommendation should highlight how the student’s cybersecurity education will be applied by the Component following graduation.**
- Endorsement from the applicant’s second- or next-level supervisor. Please note that this endorsement and the recommendation from the first-level supervisor (noted above) are two separate documents. The endorsement should highlight how the student’s cybersecurity education will be applied by the Component following graduation

Retention Program Component Office of Primary Responsibility Process

Components must provide a nomination statement for each applicant they plan to submit. Since no quotas have been allotted to the Components, it is important that application nomination statements include enough information as to why the Component is nominating the applicant. Components should consider a rank order of their students. Components should submit their nominations by **July 8, 2022**.

General questions on the DoD CySP and/or the nomination process should be addressed to the DoD CySP Program Office via email at AskCySP@nsa.gov.

Programs

Air Force Institute of Technology (AFIT)

<https://www.afit.edu/>

AFIT offers Master of Science (MS) degrees with majors in Cyber Operations, Electrical Engineering, Computer Engineering, and Computer Science. The Cyber Operations major provides an in-depth study of defensive and offensive theory, tools, and techniques associated with protection and exploitation of information-based systems. The Electrical Engineering, Computer Engineering, and Computer Science majors allow for specialization in information assurance (IA) through a subset of courses from the Cyber Operations degree program. More information about these majors can be found at <https://www.afit.edu/ENG/programs.cfm>. Doctoral degree opportunities in Electrical Engineering, Computer Engineering, and Computer Science are also available.

AFIT also offers an MS degree in Systems Engineering with a domain specialization in Cyber Systems, which provides students with the prerequisite capabilities necessary to efficiently design, analyze, deploy, protect, and exploit cyber systems (e.g., the combination of people, processes, and technology). Focus areas include database development, cyber security, network defense, data analytics, and risk management.

All students are expected to start in the Fall (August 2023) due to course sequencing. Other start dates are possible but are handled on a case-by-case basis and require a waiver.

MS in Cyber Operations, Electrical Engineering, Computer Engineering, Computer Science, and Systems Engineering (Cyber Systems):

- Full-time, in-residence only. MS students must complete thesis research and a written thesis.
- Requires 18 months for completion; an individual student's program may need to begin earlier (June) if prerequisite knowledge is needed.

PhD in Computer Science, Electrical Engineering, and Computer Engineering:

- Full-time, in-residence only. PhD students must complete a doctoral dissertation.
- Requires three years to complete; an individual student's program may be extended if prerequisite knowledge is needed.

AFIT Requirements. Listed below are the minimum eligibility requirements for participation in the CySP through AFIT. These requirements will not be waived.

- Civilian and military applicants may be of any GS or equivalent grade.
- Applicants pursuing an MS degree must have an appropriate bachelor's degree with a minimum 3.0 GPA. Applicants pursuing a PhD must have an appropriate master's degree and a 3.5 GPA.
- Required GRE scores:
 - MS degree applicants: at or above 153 verbal/148 quantitative (for tests taken on or after August 1, 2011) or at or above 500 verbal/600 quantitative (for tests taken prior to August 1, 2011).

- PhD applicants: at or above 156 verbal/151 quantitative (for tests taken on or after August 1, 2011) or 550 verbal/650 quantitative (for tests taken prior to August 1, 2011).

Questions concerning AFIT programs should be addressed to Dr. Barry Mullins at (937) 255-3636, ext. 7979; DSN 785-3636, ext. 7979, or via email at barry.mullins@afit.edu. Alternate contact is Dr. Scott Graham at (937) 255-3636, ext. 4581; DSN 785-3636 ext. 4581, or via email at scott.graham@afit.edu.

Naval Postgraduate School (NPS)

<https://nps.edu/>

NPS offers a range of technical and non-technical programs in support of cybersecurity and cyber operations. Discipline-specific and interdisciplinary degree programs allow students to study cyber operations in depth and include courses on cyber policy and strategy as well as cyber operations from a military perspective. NPS programs cover cybersecurity from both a developmental and operational perspective through courses that combine theory and practice. NPS programs allow students to apply adversarial techniques, exploitation, and cyber defense through exploratory, hand-on activities. Non-technical offerings allow students to prepare for leadership roles in defense business and management. Details regarding all NPS programs can be found at:

<https://nps.smartcatalogiq.com/en/Current/Academic-Catalog>.

A. Technical Programs

Enlisted service members may only apply for the Master's Degree programs.

Master's Degree Programs. Applicants may apply for the following degree programs: Master of Science (MS) in Computer Science (CS), MS in Cyber Systems and Operations (CSO), MS in Electrical Engineering (MSEE), MS in Engineering Science (MSES), MBA Information Systems Management, or PhD in Computer Science, Electrical and Computer Engineering, Information Sciences, or Mathematics. For most Master's programs listed, resident classes at the NPS begin in July 2023 and January 2024.

MS in Computer Science (Curriculum 368³):

- Full-time, in-residence only.
- Cyber Operations and/or Cybersecurity and Defense specialization
- Requires 8 to 9 academic quarters (24 or 27 months) to complete.
- All MS CS degree students must submit quarterly transcripts/progress reports, complete thesis research, and write a thesis.

MS in Cyber Systems and Operations (Curriculum 326):

- Full-time, in-residence only.
- Requires 7 academic quarters (21 months) to complete.
- All MS CSO degree students must submit quarterly transcripts/progress reports, complete thesis research, and write a thesis.

Master of Applied Cyber Operations (Curriculum 336):

- Full-time, in residence only.
- Eligibility: Enlisted personnel in U.S. military services with the equivalent of Navy Cryptologic Technician Networks (CTN) and Information Systems Technician (IT) ratings.
- Requires 5 academic quarters (15 months) to complete.

³ Curriculum numbers correspond to program course numbers

- All MS CSO degree students must submit quarterly transcripts/progress reports, complete thesis research, and write a thesis.

MS in Electrical Engineering (MSEE) or in Engineering Science EE (MSES (EE)): (Curriculum 590):

- Full-time, in-residence only.
- MSEE is ABET accredited. BSEE from ABET accredited program required.
- Cyber Systems specialization
- Requires 8 academic quarters (24 months) to complete.
- All MSEE and MSES(EE) degree students must submit quarterly transcripts/progress reports, complete thesis research, and write a thesis.

MBA in Information Systems Management (Curriculum 870):

- Full-time, in-residence only.
- Requires 6 academic quarters (18 months) to complete.
- It is expected that students will enroll in cyber security or cyber operations elective courses.
- All MBA in Information Systems degree students must submit quarterly transcripts/progress reports, complete an MBA Project, and write an MBA Project report.

PhD Programs. NPS offers PhD programs in cyber-related fields: Computer Science, Electrical Engineering, Information Sciences, and Mathematics.

- Full-time, in-residence only.
- Requires three years to complete.
- All PhD students must submit quarterly transcripts/progress reports, and complete both written and oral qualifying examinations as specified by the department awarding the degree. Upon completion of required examinations, students must complete dissertation research.
- Students must successfully defend their dissertation before a dissertation committee.

In addition to the Academic Catalog, department-specific details for NPS PhD programs can be found at the websites in Table 1: NPS Academic Catalog.

Table 2: NPS Academic Catalog

Department	URL
Computer Science	https://nps.edu/web/cs/welcome
Electrical and Computer Engineering	https://www.nps.edu/web/ece/
Graduate School of Defense Management	https://www.nps.edu/web/gsdm
Information Sciences	https://nps.edu/web/is/welcome
Applied Mathematics	https://nps.edu/web/math

Graduate Certificates. All NPS graduate certificates in cyber-related topics are available to resident (Res) students. Certain certificates are available to distributed learning (DL) students. Any single course can be applied to only one certificate. A cohort of at least 20

students is required for each DL certificate. Send inquiries regarding active cohorts to cyberapps@nps.edu with CySP in the subject line.

Table 3: NPS Graduate Certificate Requirements

Certificate	Dept	Credits	No. of Courses	Required Clearance	Curriculum	
					DL	Res
Cybersecurity Fundamentals	CS	13.5+	3	-	256	257
Cybersecurity Defense	CS	12	3	-	258	259
Cybersecurity Adversarial Techniques	CS	13.5	3	-	260	261
Cyber Warfare	ECE	12+	3	TS/SCI	-	288
Mathematics of Secure Communications	MA	12	3	-	-	280
Applied Cyber Operations	IS	13.5+	3	-	225	226
Cyber Operations Infrastructure	IS	15.5+	4	TS/SCI		228

B. NPS Graduate School of Defense Management (GSDM) Programs

Professional Master of Business Administration (Curriculum 860 Resident):

- Full-time, in residence.
- Cyber electives.
- Requires 4 academic quarters (12-months) to complete.
- All Professional Master of Business Administration (PMBA) resident students must submit quarterly transcripts/progress reports, complete a thesis or project, and write a thesis or project report.

Professional Master of Business Administration (Curriculum 865 DL):

- Part-time, distributed learning (DL).
- Cyber electives.
- Requires up to 20 quarters to complete (at 1 course per quarter), less with a heavier course load.
- May be completed by stacking several graduate-level certificates together.
- All PMBA DL students must submit quarterly transcripts/progress reports; complete a thesis, project, or capstone course sequence; and complete required written thesis or project reports.

Both the resident and DL PMBA programs deliver a core of defense-focused management courses to equip students with essential skills and knowledge to lead effectively in defense business and management. The programs’ flexible design provides sponsoring agencies and students opportunities to achieve their particular professional goals by selecting a combination of courses and/or certificates that meet their specific needs. The PMBA programs provides students with a solid background in management fundamentals; financial management; economic analysis; operations and logistics, and acquisition management. In a cyber-focused program, the required core GSDM courses are accompanied by a cyber-related certificate program or a set of cyber-related electives.

A notional set of certificates for the PMBA DL program is illustrated in Table 3: Notional PMBA DL Certificates.

Table 4: Notional PMBA DL Certificates

Certificate	School/ Dept	Credits	No. of Courses	Type	Curriculum
Defense Management Foundations Certificate	GSDM	12+	4	Required	192
Chief Information Officer (CIO) Management Certificate	GSDM	12+	4	GSDM Elective	198
Elective course	any	TBD	1	Elective	TBD
Cybersecurity Fundamentals	CS	13.5+	3	Cybersecurity Elective	256

The program is completed with an acceptable project, thesis, or capstone course sequence.

GSDM certificates. Selected GSDM certificates are in Table 4. Each certificate requires the completion of four courses and consists of 12 or more credits.

Table 5: Select GSDM Certificates

Certificate	Curriculum	
	DL	Res
Defense Management Foundations Certificate	192	191
Data Analytics for Defense Management		194
Chief Information Officer (CIO) Management	198	197
Principles of Analytical Management Certificate	202	201
Strategic Leadership	206	205
Leadership for Public Administrators	208	207

NPS Requirements. The minimum eligibility requirements for participation in the CySP through NPS are listed below. These requirements will not be waived.

- GS-9 grade level or higher (or equivalent); E-4 through E-9; WO-1 through WO-4; O-1 or higher (typical student is an O-3).
- MS or MBA degree program, or graduate certificate program: bachelor's degree with a minimum 3.0 GPA (on a 4.0 scale) or equivalent.
- PhD program requirements are determined individually based on colleges/universities the applicant attended, years since the applicant's last degree, work-related accomplishments, and other factors. Generally, NPS requires PhD candidates to be in the upper half of their MS program peers.
- A copy of GRE or GMAT scores.

- Students must have, or be eligible to apply for and receive, a Secret clearance upon acceptance. For certain programs, students must have a TS/SCI clearance upon acceptance.

Questions regarding specific offerings should be addressed to cyberapps@nps.edu with CySP in the subject line. General questions may be addressed to Dr. Cynthia Irvine, irvine@nps.edu.

[Joint Cyber Analytics Course \(JCAC\)](#)

JCAC is an intensive 126-day (26 week) Course of Instruction designed to prepare service members for the Cyberspace Mission. The course covers a wide variety of topics from basic computer fundamentals to advanced cyber operations (CO) topics. JCAC utilizes virtualized systems and networks to provide students with a hands-on experience that closely mimics CO scenarios that would occur in the mission. JCAC graduates support Cyber Mission Force work roles.

Uniformed military members who will graduate from JCAC or who have graduated in the past 4 years may apply to the DoD CySP and transfer JCAC credits to one of the following partner programs:

Capitol Technology University: POC: *Dr. William Butler, whbutler@captechu.edu*

- BS – Cyber and Information Security
- BS – Cyber Analytics
- BS – Management of Cyber and Information Technology
- MS – Cyber and Information Technology
- MS – Cyber Analytics
- DS – Cybersecurity

Dakota State University: POC: *Dr. Josh Pauli, josh.pauli@dsu.edu*

- BS – Cyber Operations
- MS – Applied Computer Science with Specialization in Cyber Operations

University of Maryland Global Campus: POC: *Dr. Loyce Pailen, loyce.pailen@umgc.edu*

- BS – Cybersecurity
- BS – Computer Science
- MS – Cybersecurity Technology

University of Texas at San Antonio: POC: *Prof. Glenn Dietrich, Glenn.Dietrich@utsa.edu*

- BBA – Cybersecurity
- BS – Computer Science – concentration in computer security
- BS – Computer Science – concentration in cyber operations
- MS – IT concentration in Cybersecurity
- MS – Management of Technology
- PhD – Cyber Security (resident only)

University of West Florida: POC: *Dr. Eman El-Sheikh, eelsheikh@uwf.edu*

- BS – Computing and Information Science – concentration in Cybersecurity

The DoD CySP is utilizing a partnership program between specific National Centers of Academic Excellence in Cybersecurity (NCAE-Cs) and the JCAC program. **The DoD CySP cannot assist interested military service members with acceptance to the JCAC program.** Additional NCAE-Cs may be added in the future.

DoD CySP Community College Program

The Fiscal Year 2018 National Defense Authorization Act (Public Law 115-91) required the DoD to establish a community college scholarship program within the DoD CySP. Permanent DoD civilian and uniformed employees seeking to enhance their cyber skills and knowledge may pursue an associate degree at a community college or college/university offering 2-year degrees designated as a National Center of Academic Excellence in Cyber Security (NCAE-C).

Students participating in this program will have up to four years to complete an associate degree. Ideal candidates will have earned previous academic credits that can be applied toward completing their degree. Most programs offer experienced-based credits. In addition, schools may offer credit for specific technical training received. An excellent resource is the Military Occupational Specialty Crosswalk maintained by CyberWatch West: <http://cyberwatchwest.org/index.php/faculty-141/mos-pathways>.

The DoD CySP Program Office can assist the applicant with identifying an institution's point of contact.