Avue

OMB Control Number: 0704-0486
DoD Cyber Scholarship Program (CySP)

Cybersecurity is considered so important to our national defense that a formal DoD Cyber Scholarship Program (CySP) was established by the National Defense Authorization Act for 2001 (Public Law 106- 398). The purpose is to promote the education, recruitment, and retention of rising second-year NCAE-C community college, junior and senior undergraduate, and graduate/doctoral students in cybersecurity studies. In 2018, the program was renamed the DoD Cyber Scholarship Program (DoD CySP).

The DoD is seeking rising second-year NCAE-C community college, junior and senior (third and fourth year) undergraduate, and graduate/doctoral students who are interested in full-ride scholarships for concentrated studies in cybersecurity and other cyber-related disciplines. Click here for application background and requirements information.

To be considered for the DoD Cyber Scholarship Program, students must agree to certain academic standards and conditions of employment. The OF612 Supplemental Statement of General Academic and Employment Conditions describes those conditions. Read this statement carefully (click OF612). Before submitting this application, you will be required to certify that you understand each of the academic and employment conditions.

NOTE: Current DoD civilians and active duty military may not use this portal to apply for the DoD CySP. Please contact the DoD CySP Program Office via email at AskCySP@nsa.gov or by telephone at (410) 854-6206 for more information about the Retention Program.

Please Read These Instructions.
After You Answer the Acknowledgement Questions
You May Begin Filling Out Your Application.

How to Apply
Only students at designated National Centers of Academic Excellence in Cybersecurity (Cyber Defense Education, Research, and Operations), hereinafter referred to as NCAE-Cs, may apply. Click here to review the list of schools for clarification.

Note: Undergraduate students selected must attend full-time.
Online programs are allowed

Review all application instructions and materials included with this announcement. Pay close attention to the mandatory conditions of financial assistance and employment.

Check with the identified Point of Contact for your college or university to find out what you must do to apply and to obtain an augmented application package if your school requires one. (Application due dates and requirements may vary from school to school.) Each NCAE-C has designated a campus liaison, point of contact, or Principal Investigator (PI), for CySP management and administration. The above reference website provides known points of contact for the current NCAE-Cs. You are responsible for identifying the appropriate PI for the CySP on your campus.

DO NOT SUBMIT YOUR APPLICATION TO THE DOD. Upon completion of your online application, it will be submitted directly to the appropriate Point of Contact for your college or university.

PRIVACY ACT STATEMENT
Authority for collecting information requested on the DoD Cyber Scholarship Program Application is contained in 5 U.S.C. Section 4101-4121, 10 U.S.C. §2200, Executive Order 13111, Executive Order 11348, as amended, and DoD Directive 8500.2. DoD's Blanket Routine Uses (found at Appendix C of 32 CFR Part 310) and the specific uses found in GNSA27 apply to this information. The requested information will be used to determine eligibility for the Cyber Scholarship Program. Disclosure of the requested information is voluntary. However, failure to provide the requested information will prevent the processing of your application and the determination of your eligibility for the Cyber Scholarship Program.

AGENCY DISCLOSURE NOTICE
The public reporting burden for this collection of information is estimated to average 5 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to the Department of Defense, Washington Headquarters Services, Executive Services Directorate, Directives Division, **OSD.CyberspaceWorkforce-TAG@mail.mil**, [OMB Control Number (0704-0486)]. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

EQUAL EMPLOYMENT OPPORTUNITY
The Department of Defense is an Equal Opportunity Employer. All qualified persons shall receive consideration for this opportunity without regard to political, religious, labor organization affiliation or non-affiliation, marital status, race, color, sex, national origin, non-disqualifying physical disability, age, or sexual orientation.

ACKNOWLEDGEMENTS

To be considered for the DoD Cyber Scholarship Program (CySP), you must agree to certain academic standards and conditions of employment. Please read OF612, Supplemental Statement of General Academic and Employment Conditions before acknowledging the following (click OF612).

I understand that, before being hired, the appointing agency (the specific DoD Agency requesting to hire me) will ask me to complete a Declaration of Federal Employment or other agency or component specific form to determine my suitability for federal employment and to authorize a background investigation of my suitabilty. I understand that I will be asked to sign and certify the accuracy of all the information in my application. I understand a false statement in any part of my application may result in not being hired; may be cause for firing after I begin work; or may be cause for being fined or jailed.

I understand that I will be required to obtain and maintain eligibility for a security clearance in order to receive financial (scholarship) assistance or an appointment under the DoD CySP, which may include undergoing drug and polygraph tests and providing potentially sensitive information about my financial circumstances and any arrests and/or convictions for offenses of any kind.

I agree to be mobile. I understand that I may have to travel to my duty station for summer internships and/or final service placement, which could be in another city and/or state. I also understand that I may have to accept assignments in different organizations, assignments in different functional areas, and assignments in different geographic areas during my internship, if applicable, AND during my incumbency of any permanent, full-time position to which I am converted on program completion.

Should I receive financial assistance (scholarship) under the DoD CySP, I understand that I may only accept up to $6,000 per academic year in additional funding sources (scholarships, awards, fellowships, and/or grants). I understand that the DoD CySP must pay 100% of my tuition and fees. Additional funding may be used for books, housing, meal plans, supplies, transportation, and other miscellaneous academic fees/services. I understand loans obtained by me (the student) do not count towards the $6,000 cap, as I am required to pay them back.

Should I receive financial assistance (scholarship) under the DoD CySP, I understand that I am obligated to work for the DoD, either as a civilian employee or active duty military personnel. As a civilian employee, my period of obligated service will be one calendar year for each academic year, or partial year, for which financial assistance (scholarship) is received. For military service, my service obligation will be a minimum of 4 years of active duty but may be longer than 4 years, depending on the occupational specialty and type of enlistment or commissioning program selected.

If I receive financial assistance (scholarship) under the DoD CySP, I understand that I must reimburse the United States should I voluntarily terminate my appointment under the CySP; decline or refuse to honor my commitment to accept permanent employment; or voluntarily terminate permanent employment before I have fulfilled my period of obligated service.

I have read, understand, and agree with all of the academic standards and conditions of employment outlined and described in OF612 Supplemental Statement of General Academic and Employment Conditions. (click OF612).

Personal Information

* First Name

Middle Name

* Last Name

* Current Address

* City

* State/Province

Other State (if applicable)

* Country

* ZIP/Postal Code

* Cell Phone

Secondary Phone

* Email Address

* Confirm Email Address

*** Mailing Address:**

*** City:**

*** State/Province:**

Other State:

*** Country:**

*** Zip/Postal Code:**

*** Student School Email Address:**

Demographics

Provision of demographic information is voluntary; there are no consequences associated with non- or partial response to these questions. Any demographic information you provide will be kept confidential. It will not be reflected on your application or disclosed to reviewers as a part of the standard review and selection process but will be used for statistical and reporting purposes only. There are no adverse consequences if you do not respond.

Ethnicity, Race Identification, and Disability Information Privacy Act Statement and Explanation on How This Data Is Used

Ethnicity

Are you Hispanic or Latino (a person of Cuban, Mexican, Puerto Rican, South or Central American, or other Spanish culture or origin, regardless of race.)? Yes / No / Decline to Answer

Race and National Origin Identification

Select the racial category or categories with which you most closely identify by checking the boxes. (For equal opportunity reporting purposes data is aggregated - if you check more than one box, you will be reported in the category "Two or More Races.")
American Indian or Alaska Native
Asian
Black or African American
Native Hawaiian or Other Pacific Islander
White
Decline to answer

Gender Female / Male / Decline to answer

Disability

Do you have a disability (a physical or mental impairment which substantially limits one or more major life activities)? Yes / No / Decline to answer

Blindness
Convulsive Disorders
Deafness
Distortion of Limb or Spine
Mental Illness
Mental Retardation
Complete Paralysis
Partial Paralysis

My disability is not one of those listed
I do not have a disability
Decline to answer

General Requirements

I am a U.S. citizen. Yes / No

At the start of FALL semester of Academic Year 2022-2023, I will be 18 years of age or older. Yes / No

Selective Service registration is required by law as the first part of a fair and equitable system that, if authorized by the President and Congress, would rapidly provide personnel to the Department of Defense while at the same time providing for an Alternative Service Program for conscientious objectors.

I am a male born after December 31, 1959 Yes / No

I have registered with the Selective Service. *If you have registered but do not know your registration number, click here.*

My confirmation number is (ex: 12-1234567-1)

Applicants selected for the DoD CySP will be required to perform a service obligation; therefore, applicants must be free from prior obligations that also carry a service obligation.

I currently do not have a service obligation with another sponsored program (Federal or commercial). True / False

Full-time Federal employees are not eligible to participate in the recruitment portion of the DoD CySP. Processing for a full-time position will not preclude you from applying, but it may cause you to become ineligible if you are selected for the full-time position.

I am currently processing for a full-time Federal position. Yes / No

Summer internships are a great way for applicants to gain experience but are not required in order to apply for the DoD CySP. Please indicate if you are applying for a Federal Summer Internship.

I am currently processing for a Federal summer internship position. Yes / No

Academic Requirements

I am currently enrolled or accepted for enrollment in a National Centers of Academic Excellence in Cybersecurity (NCAE-C) academic institution. Yes / No

If your NCAE-C institution is not listed among the choices in the application, please contact the DoD CySP Program Office at AskCySP@nsa.gov.

* Select the NCAE-C academic institution you plan to attend should you be selected for a scholarship. (It can be your current institution or a school you have applied to for future placement).
If you are selected for a scholarship and intend to use that scholarship at an institution other than your current school, you may list any schools you are applying to here.

Map / Pick List

My current GPA is one of the following (no rounding):
3.2 or higher for Community College students; OR
3.2 or higher for Undergraduate students; OR
3.5 or higher for Graduate students

My current GPA is: (Enter GPA: X.XX; no rounding). GPA MUST match transcripts.

School Grading Scale: ⓘ **4.0 to 0.0**

TRANSCRIPTS

MANDATORY: Attach current transcripts that validate the GPA you identified above.

These transcripts can be unofficial or official. Failure to attach your transcripts will deem the application package to be incomplete, and you will not be considered for the DoD CySP. If you attach an unofficial transcript and are selected to receive a scholarship, you will be required to provide official transcripts to the DoD CySP Program Office.

- Transcripts may be official or unofficial but must be generated by the academic institution; transcripts may not consist of an applicant-generated "grade report" or similar document.
- Attach ONLY transcripts that validate the GPA you identified above. Do NOT attach other educational transcripts unless you are cross-enrolled in a joint-degree program with a merged transcript.
- Ensure your attached transcript is not password protected.
- FAILURE TO ATTACH A READABLE SCHOOL-GENERATED TRANSCRIPT WILL RESULT IN DISQUALIFICATION.

Degree-Related Requirements

In the FALL of Academic Year 2022-2023, I will have at least one full academic year remaining in a degree program(s). Yes / No

Anticipated Final Graduation Date (MM/DD/YYYY):

I am pursuing a course of study and/or have a declared major in one of the scientific, technical, or managerial disciplines related to cyber or with a concentration in cybersecurity. Yes / No

Identify Declared Major
Select the scientific, technical, and managerial disciplines related to computer and network security and cybersecurity from the lists below.

Cybersecurity Functions: (select all that apply)

System/network administration and operations
Systems security engineering
Information assurance systems and product acquisition
Cryptography
Threat and vulnerability assessment, to include risk management
Web Security
Operations of computer emergency response teams
Computer Forensics
Defensive information operations
Critical information infrastructure assurance

Cyber-related academic discipline(s) with concentrations in cybersecurity: (select all that apply)

Biometrics
Business - Management
Business - Administration
Computer - Crime Investigations
Computer - Engineering
Computer - Forensics
Computer - Information Science
Computer - Information Systems
Computer - Programming
Computer - Science
Computer - Systems Analysis
Critical Information Infrastructure Assurance
Cyber - Defense
Cyber - Operations
Cyber - Security
Cyber - Policy
Cryptography
Database Administration
Data Management
Data Science
Digital and Multimedia Forensics
Electrical Engineering
Electronics Engineering
Information Assurance
Systems and Product Acquisition
Information Security (Assurance)
Information Systems
Information Technology - Acquisition
Information Technology - Program/Project Management
Mathematics
Network Administration and Operations
Network Management
Operation of Computer Emergency Response Teams
Software Engineering
Systems Security Engineering
Threat and Vulnerability Assessment, to include Risk Management
Web Security
Other similar disciplines - Identify other declared major in the text box provided below

Credits Earned to Date for Declared Major:

Credits Needed to Graduate for Declared Major:

In the FALL of academic year 2022-2023, I will have already completed work towards a higher degree; i.e., the first year of an associate's degree; **OR** the first two years of an undergraduate degree program; **OR** a bachelor's degree; **OR** a master's degree. Yes / No

Indicate the degree level you will enter in the FALL of academic year 2022-2023.
Community College
Bachelor's
Master's
PhD/Doctorate

Identify the declared major for the degree level/program you are requesting to be supported by the DoD CySP if selected: Junior Year / Senior Year / Senior Year-1st Year Master's

Declared Major Cybersecurity

My degree program is: (select one) Online In-Person / Online / Hybrid

Professional Summary

Provide a one or two sentence overview of your short-term professional goals and explanation of why you're the best candidate to qualify for this scholarship.:

Education

School Name	Type	Degree	Degree Field	GPA	Date Received

Cyber Coursework

In order to qualify for a CySP scholarship, you must be pursuing a course of study and/or have a declared major in one of the scientific, technical, or managerial disciplines related to cyber or with a concentration in cybersecurity. List coursework you have completed that are related to computer and network security and cybersecurity. Please limit your list to a maximum of **10 courses**.:

Skill Set / Certifications

Technical Proficiencies

List technical proficiencies, including platforms, networks, languages, and tools used in your past positions.:

Certifications

Department of Defense Approved Certifications

From the list below, select all certifications you have acquired. Provide the date the certification was awarded/received (mandatory); and the expiration date of the certification (if known)
A+ - A+ Certification (CompTIA)
CAP - Certified Authorization Professional [(ISC)2]
CASP+ - CompTIA Advanced Security Practitioner
CCISO - Certified Chief Information Security Officer (EC-Council)
CCNA CyberOps - Cisco Certified Network Associate CyberOps Certification
CCNA-Security - Cisco Certified Network Associate-Security
CCNP-Security - Cisco Certified Network Professional-Security
CCSP - Certified Cloud Security Professional [(ISC)2]
CEH - Certified Ethical Hacker [EC-Council]
CFR - CyberSec First Responder (CertNexus)
CHFI - Computer Hacking Forensic Investigator [EC-Council]
CISA - Certified Information Systems Auditor [ISACA]
CISM - Certified Information Security Manager [ISACA]
CISSP - Certified Information Systems Security Professional [(ISC)2]
CISSP Associate - Certified Information Systems Security Professional Associate [(ISC)2]
CISSP-ISSAP - Certified Information Systems Security Professional-Information Systems Security Architecture Professional [(ISC)2]
CISSP-ISSEP - Certified Information Systems Security Professional-Information Systems Security Engineering Professional [(ISC)2]
CISSP-ISSMP - Certified Information Systems Security Professional-Information Systems Security Management Professional [(ISC)2]
Cloud+ - CompTIA Cloud+
CND - Certified Network Defender [EC-Council]
CSA+ Certification - CompTIA Cybersecurity Analyst
CSSLP - Certified Secure Software Lifecycle Professional [(ISC)2]
CySA+ (CSA+) - CompTIA Cybersecurity Analyst
GCED - GIAC Certified Enterprise Defender
GCFA - GIAC Certified Forensic Analyst
GCFE - GIAC Certified Forensic Examiner
GCIA - GIAC Certified Intrusion Analyst
GCIH - GIAC Certified Incident Handler
GICSP - Global Industrial Cyber Security Professional
GSEC - GIAC Security Essentials Certification
GSLC - GIAC Security Leadership Certification
GSNA - GIAC Systems and Network Auditor
Network+ - Network+ (CompTIA)
PenTest+ - CompTIA PenTest+
SCYBER - Cybersecurity Specialty Certification (Cisco)
Security+ - Security+ (CompTIA)
SSCP - Systems Security Certified Practitioner [(ISC)2]

Other Certifications

From the list below, select all certifications you have acquired. Provide the date the certification was awarded/received (mandatory); and the expiration date of the certification (if known).

If you have certifications other than what is listed here, select 'Other' and list the certification(s) in the text box provided, along with the date awarded (mandatory) and expiration date (if known) for each certification you list.
ABCP - Associate Business Continuity Professional
AWS Certified Solutions Architect - Associate
AWS Certified Solutions Architect - Professional
CBCP - Certified Business Continuity Professional
CBRM - Certified Business Resilience Manager
CCFP - Certified Cyber Forensics Professional [(ISC)2]
CEPT - Certified Expert Penetration Tester
CFCP - Certified Functional Continuity Professional
CIH - Certified Incident Handler
Cisco Certified CyberOps Associate Certification
CNDA - Certified Network Defense Architect [EC-Council]
CPT - Certified Penetration Tester
CPTC - Certified Penetration Testing Consultant
CPTE - Certified Penetration Testing Engineer
CRISC - Certified in Risk and Information Systems Control [ISACA]
CSCU - Certified Security Computer User [EC-Council]
CSTA - Certified Security Testing Associate
CVP - Certified Virtualization Professional
ECIH - EC-Council Certified Incident Handler
ECSA - EC-Council Certified Security Analyst
ECSP Java - EC-Council Certified Secure Programmer Java
ECSP .Net - EC-Council Certified Secure Programmer .Net
EDRP - EC-Council Disaster Recovery Professional
FAC-C-DS - Federal Acquisition Certification in Contracting-Digital Services
GASF - GIAC Advanced Smartphone Forensics
GAWN - GIAC Assessing and Auditing Wireless Networks
GCCC - GIAC Critical Controls Certification
GCDA - GIAC Certified Detection Analyst
GCIP - GIAC Critical Infrastructure Protection
GCPM - GIAC Certified Project Manager
GCSA - GIAC Cloud Security Automation
GCTI - GIAC Cyber Threat Intelligence
GCUX - GIAC Certified UNIX Security Administrator
GCWN - GIAC Certified Windows Security Administrator
GDAT - GIAC Defending Advanced Threats
GDSA - GIAC Defensible Security Architecture
GEVA - GIAC Enterprise Vulnerability Assessor
GISF - GIAC Information Security Fundamentals
GISP - GIAC Information Security Professional
GLEG - GIAC Law of Data Security & Investigations
GMOB - GIAC Mobile Device Security Analyst
GMON - GIAC Continuous Monitoring Certification
GNFA - GIAC Network Forensic Analyst
GOSI - GIAC Open Source Intelligence
GPEN - GIAC Penetration Tester
GPPA - GIAC Certified Perimeter Protection Analyst
GPYC - GIAC Python Coder

GREM - GIAC Reverse Engineering Malware
GRID - GIAC Response and Industrial Defense
GSE - GIAC Security Expert
GSE-Compliance - GIAC Security Expert-Compliance
GSE-Malware - GIAC Security Expert-Malware
GSSP-.NET - GIAC Secure Software Programmer-.NET
GSSP-JAVA - GIAC Secure Software Programmer-Java
GSTRT - GIAC Strategic Planning, Policy, and Leadership
GWAPT - GIAC Web Application Penetration Tester
GWEB - GIAC Certified Web Application Defender
GXPN - GIAC Exploit Researcher and Advanced Penetration Tester
HCISSP - HealthCare Information Security and Privacy Practitioner [(ISC)2]
LPT (Master) - Licensed Penetration Tester (Master) [EC-Council]
MBCP - Master Business Continuity Professional
MCSA -Microsoft Certified Solutions Associate - Windows Server 2012
MCSA -Microsoft Certified Solutions Associate - Windows Server 2016
MCSE - Microsoft Certified Solutions Expert - Cloud Platform and Infrastructure
MCSE - Microsoft Certified Solutions Expert - Data Management and Analytics
MCSE - Microsoft Certified Solutions Expert - Mobility
MCSE - Microsoft Certified Solutions Expert - Productivity
MCSE - Microsoft Certified Solutions Expert - Server Infrastructure
MMAD - Master Mobile Application Developer [Logical Operations]
OSCP - Offensive Security Certified Professional
PgMP - Program Management Professional [PMI]
PMP - Project Management Professional [PMI]
SCNA - Security Certified Network Architect [SCP-Security Certified Program]
SCNP - Security Certified Network Professional [SCP-Security Certified Program]
SCNS - Security Certified Network Specialist [SCP-Security Certified Program]
SSAP - SANS Security Awareness Professional Credential
Other Certification - List in text box provided below.

Work History

Job Title	Employer	Dates	Salary	Federal Job?	Pay Plan-Series-Grade

Location: (State, City, Country)

Supervisor Name: **Phone:** **Email:**

Key Projects

Provide information about key projects in which you have been involved. Include extracurricular activities that help you stand out from among other student applicants. Don't limit yourself to only including paid work experience. Include relevant volunteer work, community organizations, roles, societies, language proficiency, and prior military experience that demonstrate your ability to do the job.:

*** Have you participated in a STARTALK language summer program? Yes / No**

*** Have you participated in the GenCyber cybersecurity camp program? Yes / No**

Recognitions, Honors, and Awards

My recognitions, honors, and awards include::

References

Reference Name	Relation To Applicant	Title	Company	City,State
	PHONE:	**EMAIL:**		
	PHONE:	**EMAIL:**		
	PHONE:	**EMAIL:**		

Letters of Reference

Attach Reference Letter #1 here

* REFERENCE LETTER #1 (from a current or former faculty member, mentor, or employer)

REFERENCE LETTER #2 (from a current faculty member [or a most current faculty member]). Reference Letter from current faculty member (or a most current faculty member) must be sent directly to the CySP Scholarship program. Please provide us the following information regarding your recommender:

* Name of Recommender for Reference Letter #2 (Current Faculty Member):

* Title of Recommender:

* Email Address of Recommender:

* Phone Number of Recommender:

Note to Applicant

It is your responsibility to contact your second recommender and request that they prepare and submit a letter of recommendation on your behalf. They must submit this letter of recommendation directly to the DoD CySP Program Office at AskCySP@nsa.gov.

Click this link to download an instructional PDF to provide to your second recommender, detailing how to prepare and submit the letter of recommendation.

Competencies

1. Knowledge of the techniques of the cybersecurity discipline, including encryption, access control, physical security, training, threat analysis, and authentication.:

2. Knowledge of the human factors in cybersecurity, including human computer interaction, design, training, sabotage, human error prevention and identification, personal use policies, and monitoring.:

3. Ability to identify and analyze problems, distinguish between relevant and irrelevant information to make logical decisions, and provide solutions to individual and organizational problems.:

4. Ability to consider and respond appropriately to the needs, feelings, and capabilities of different people in different situations; is tactful, compassionate and sensitive, and treats others with respect.:

5. Ability to make clear and convincing oral presentations to individuals or groups; listens effectively and clarifies information as needed; facilitates an open exchange of ideas and fosters an atmosphere of open communication. :

6. Ability to express facts and ideas in writing in clear, convincing, and organized manners appropriate to the audience and occasion.:

Military Service & Veterans' Preference

Military Service

Select the appropriate response:

○ I served in the United States Armed Forces.
○ I am the spouse, un-remarried widow/widower, or parent of a deceased or disabled U.S. veteran who has been administratively deemed eligible for derivative entitlement to veterans' preference.
○ No Response / Not Applicable

Branch of Service:

Date of Service:
From: MM/DD/YYYY X To: MM/DD/YYYY X

Characterization of Service Listed on DD214

○ Honorable (including General (Under Honorable Conditions) discharges)
○ All Others
○ Not applicable (for applicants administratively deemed eligible for derivative entitlement to veterans preference)

Veterans' Preference Eligibility

If you served on active duty in the United States Military and were separated under honorable conditions, you may be eligible for veteran's preference. For further details, visit the Office of Personnel Management website at: https://www.fedshirevets.gov/job-seekers/veterans-preference/

Military retirees at the rank of major, lieutenant commander, or higher (04 and above) are not eligible for veterans' preference unless they are qualifying disabled veterans. This restriction does not apply to Reservists who do not begin drawing military retired pay until age 60.)

Are you eligible for veterans' preference?

Yes
No

Applicants claiming veterans' preference: Attach DD Form 214, Certificate of Release or Discharge from Active Duty, and other documents that validate preference eligibility. You can confirm attachments on the "Review Supporting Documents" screen.

no file selected

If eligible, select the category in which you qualify.

"0" Point (SSP) Preference

Veterans qualify for this category if discharged based on sole survivorship in a family where the father or mother or one or more siblings:

1. Served in the armed forces, *and*
2. Was killed, died as a result of wounds, accident, or disease, is in a captured or missing in action status, or is permanently 100 percent disabled or hospitalized on a continuing basis (and is not employed gainfully because of the disability or hospitalization), *where*
3. The death, status, or disability did not result from the intentional misconduct or willful neglect of the parent or sibling and was not incurred during a period of unauthorized absence.

I am a veteran whose discharge from active duty was based on sole survivorship.

"5 Point" (TP) Preference:

Veterans qualify for this category on the basis of service during a specific time or place, or by receiving certain medals or participating in campaigns or expeditions for which a campaign medal has been authorized. These preference eligibles do not have a disability rating.

I am an honorably separated veteran who served on active duty (not active duty for training) in the Armed Forces:

For 180 or more consecutive days, any part of which occurred after January 31, 1944 and before October 15, 1976; *or*

During the Gulf War period beginning August 2, 1990, and ending January 2, 1992; *or*

For 180 or more consecutive days, any part of which occurred during the period beginning September 11, 2001, and ending on August 31, 2010, the last day of Operation Iraqi Freedom; *or*

In a campaign or expedition for which a campaign medal has been authorized, such as Operations Enduring Freedom and Iraqi Freedom, Kosovo, Bosnia and Herzegovina, Haiti, Somalia, etc. You must have received the expeditionary medal to qualify.

"10 Point" (CPS, CP, XP) Preference:

Veterans qualify for this category based on service-connected disability or through the award of the Purple Heart medal. Spouses, widows/widowers or parents of a deceased or disabled preference-eligible veteran may qualify for derivative preference. Derivative preference may not be claimed if the veteran is living and is qualified for federal employment. Applicants claiming this level of preference must attach SF-15 and any other substantiating documents. See www.opm.gov/forms/pdf_fill/SF15.pdf for details.

no file selected

(CPS) I am an honorably separated veteran who has a present service-connected disability or who is receiving compensation, disability retirement benefits, or pension from the military or the Department of Veterans' Affairs and I have a disability rating of 30% or more. *or*

(CP) I am an honorably separated veteran who has a present service-connected disability or who is receiving compensation, disability retirement benefits, or pension from the military or the Department of Veterans' Affairs and I have a disability rating of 10% but less than 30%. *or*

(XP) I am an honorably separated veteran who has a present service-connected disability rating of less than 10% or who received a Purple Heart *or*

(XP) I am the unmarried widow/widower of a deceased veteran who qualifies for derivative preference or I am the spouse/parent of a veteran who died in service or who is permanently and totally disabled.

OTHER MILITARY SERVICE / INTEREST

I am a current member of the National Guard or a Reserve Unit.

Yes
No

I would be interested in active duty military service as a means to meeting my obligated service requirements.

Yes
No

Agency Preferences

The DoD **does not guarantee** that your preferences for agency assignment under the DoD CySP, or in a permanent position to which you are subsequently converted, can be honored. Your preferences will be taken into account, along with all other relevant factors such as: mission, functional, and staffing requirements; the exigencies of service; the availability of funds; and, any hardships you may demonstrate.

Nonetheless, your agency preferences are important to the department. Therefore, you may specify up to **three** (3) agency preferences below, if you wish. You are not required to complete these preference selections. However, if you do so, please select and designate in rank order of preference (1-2-3).

If you select "Other" as one of your ranked choices, please provide the name of the agency in the text box provided.

For information on DoD Agencies, you may view the following website:https://www.defense.gov/Resources/Military-Departments/A-Z-List/

Department of Defense (DoD)
Defense Information Systems Agency (DISA)
Defense Intelligence Agency (DIA)
Defense Manpower Data Center (DMDC), Defense Human Resources Activity
Defense Media Activity (DMA)
Defense Security Cooperation Agency (DSCA)
Defense Technical Information Center (DTIC)
Director of Operational Test and Evaluation (DOT&E)
Missile Defense Agency (MDA)
National Reconnaissance Office (NRO)
National Security Agency (NSA)
Office of the Secretary of Defense Microelectronics Activity (DMEA) - Cybersecurity and Compliance Branch
U.S. Cybercom J2 (USCYBERCOM-J2)
USSTRATCOM C4 Systems Directorate / 67th Cyberspace Wing (USSSTRATCOMC4)
United States Special Operations Command

Department of the Air Force (AF)
Air Combat Command (ACC)
US Air Force 177th Red Team (USAF177)
USAF 318th Cyberspace Operations Group

Department of the Army (AR)
U.S. Army 780th Military Intelligence Brigade (MI BDE)
U.S. Army Combat Capabilities Command (CCDC) - Futures Command
U.S. Army Combat Capabilities Development Command (DEVCOM) Data & Analysis Center
U.S. Army Cyber Command (USARCYBER)
U.S. Army Cyber Protection Brigade
U.S. Army Futures Command (AFC)
U.S. Army HQ Network Enterprise Technology Command
U.S. Army HQDA CIO G-6 (DCSG-6)
U.S. Army Network Enterprise Technology Command (NETCOM)
U.S. Army PEO Simulation, Training, and Instrumentation / Threat Systems Management Office Redstone Arsenal (US Army TSMO)

Department of the Navy (NV)
Commander, Naval Air Systems Command (COMNAVAIRSYSCOM)
NAVFAC Engineering & Expeditionary Warfare Center (EXWC)
NAVFAC Headquarters - DC Navy Yard
Naval Air Systems Command (NAVAIR)
Naval Air Systems Command (NAVAIR) - Office of the CIO (OCIO)
Naval Air Warfare Center Weapons Division (NAWCWD)
Naval Air Warfare Center Weapons Division (NAWCWD) Cyber R&D
Naval Facilities Engineering Systems Command (NAVFAC)
Naval Information Warfare Center Atlantic (NIWC Atlantic)
Naval Information Warfare Center Pacific (NIWC Pacific)
Naval Sea Systems Command (COMNAVSEASYSCOM)
Naval Sea Systems Command - Warfare Centers - NSWC - Port Hueneme Division
Naval Supply Systems Command (NAVSUP) - Business Systems Center
Naval Supply Systems Command (NAVSUP) - Weapon Systems Support
Naval Surface Warfare Center (NAVSURFWARCEN)
Naval Surface Warfare Center Dahlgren Division (NSWCDD)
Naval Surface Warfare Center, Crane Division (NSWCCD)
Naval Surface Warfare Center, Philadelphia (NSWCPD)
Naval Undersea Warfare Center (NUWC)
Navy Fleet Human Resource Office
U.S. Naval Academy (USNA)
US Navy Cyber Warfare Test and Evaluation Branch Head (USNCWTEB)

U.S. Marine Corps (MC)
Marine Corps Cyberspace Operations Group (MCCOG)
Marine Corps Systems Command (MARCORSYSCOM)
U.S. Marine Corps Forces Cyberspace Command (MARFORCYBERCOM)
USMC Information (DC I), Command, Control, Computers and Communication (IC4), Compliance (HQMC-CYBER)

Cyber Work Roles of Interest

The following list describes the overall categories of cybersecurity work in the Federal government. Various Work Roles are grouped in these categories. For a description of each category and Work Role, click the information icon beside each item.

Select the Work Roles in which you are interested. Select as many as you wish.

Analyze - Work Roles
All-Source Analyst (111)
Mission Assessment Specialist (112)
Exploitation Analyst (121)
Target Developer (131)
Target Network Analyst (132)
Target Reporter (133)
Warning Analyst (141)
Multi-Disciplined Language Analyst (151)

Investigate - Work Roles
Forensics Analyst (211)
Cyber Defense Forensics Analyst (212)
Cyber Crime Investigator (221)

Collect and Operate - Work Roles
All-Source Collection Manager (311)
All-Source Collection Requirements Manager (312)
Cyber Operator (321)
Access Network Operator (321)
Interactive Operator (322)
Cyber Intel Planner (331)
Cyber Ops Planner (332)
Partner Integration Planner (333)

Operate and Maintain - Work Roles
Technical Support Specialist (411)
Database Administrator (421)
Data Analyst (422)
Knowledge Manager (431)
Network Operations Specialist (441)
System Administrator (451)
Systems Security Analyst (461)

Protect and Defend - Work Roles
Cyber Defense Analyst (511)
Cyber Defense Infrastructure Support Specialist (521)
Cyber Defense Incident Responder (531)
Vulnerability Assessment Analyst (541)

Securely Provision - Work Roles
Authorizing Official (611)
Security Control Assessor (612)
Software Developer (621)
Secure Software Assessor (622)
Information Systems Security Developer (631)
Systems Developer (632)
Systems Requirements Planner (641)
Enterprise Architect (651)
Security Architect (652)
Research & Development Specialist (661)
System Testing and Evaluation Specialist (671)

Oversee and Govern - Work Roles
Cyber Instructional Curriculum Developer (711)
Cyber Instructor (712)
Information Systems Security Manager (722)
COMSEC Manager (723)
Cyber Legal Advisor (731)
Privacy Compliance Manager (732)
Cyber Workforce Developer and Manager (751)
Cyber Policy and Strategy Planner (752)
Program Manager (801)
IT Project Manager (802)
Product Support Manager (803)
IT Investment/Portfolio Manager (804)
IT Program Auditor (805)

Languages

Click the "Add" button to enter information about fluency in languages other than English. If you do not have fluency in other languages, you may continue without entering anything here by clicking the Save & Continue button. If you are fluent in other languages, add a separate entry for each language. Continue until you have listed all of your languages. A summary of your results will appear in the table below. After you have entered information, the table will populate and, should you need to, you may select any entry by clicking on the check box next to it, and then click the Edit or Delete buttons to make any adjustments.

Language	Oral Proficiency	Written Proficiency	Listen Proficiency

Computer Programming Languages

Select all computer programming languages you have used, and your proficiency level in each.

When considering your programming language proficiency level, use the following scale to choose the level that best describes your skills:

- **Dabbled In:** I have read or completed tutorials in this programming language, and with additional training I could perform programming language functions under supervision or with guidance from peers.
- **Basic User: I** can perform computer programming language functions under supervision or under dedicated/personalized guidance from peers.
- **Intermediate User:** I can perform computer programming language functions without supervision or guidance from peers, or with minimal effort from peers.
- **Proficient User:** I am fully independent and can demonstrate computer programming skills corresponding to a high expertise level according to the majority of other users of the language.
- **Expert User:** I have developed an implied and deep knowledge through practical experience, and my programming language skill level allows me to approach a situation analytically and intuitively without rigid guidelines.

C Language
C#
C++
COBOL
HTML
Java
JavaScript
Objective-C
PHP
Python
Ruby / Ruby on Rails
SQL
Swift
Other - Specify below

Security Clearance

If you have ever held a security clearance, issued by a U.S. Government agency, please select the highest level of clearance you have been awarded.

Confidential
Secret
Top Secret
Sensitive Compartmented Information (DCID/14)
Q (Atomic Energy Act)
L (Atomic Energy Act)
Other
Not Applicable; I have not held a U.S. Government-issued security clearance

Attached Documents

Instructions
This section permits applicants to review previously attached documents or attach missing documents prior to submission to ensure their application is complete.

Listed below are the documents that must be attached to this online application in order for your application package to be considered complete.

Please be aware that your NCAE-C is required by the DoD to participate in the evaluation of your application. To fulfill its responsibilities, your NCAE-C may require that you obtain and submit information and/or materials in addition to those required in the application package. Any written information or material that your NCAE-C requires shall become the NCAE-C Supplement to your application and must be included in the final application package that your school transmits to the DoD in order for you to receive consideration. **Therefore, if your NCAE-C requires additional documents for eligibility or evaluation purposes, attach those documents below.**

FAILURE TO ATTACH THE REQUIRED DOCUMENTS PRIOR TO CERTIFYING AND SUBMITTING THIS APPLICATION WILL DEEM YOUR APPLICATION TO BE NON-RESPONSIVE, AND IT WILL NOT BE CONSIDERED.

MANDATORY DOCUMENTS: (All Applicants)

1. Official (certified) transcripts that validate the GPA you identified in the application.
2. Letters of reference (2 for New Applicants; 1 for Returning CySP Students).

OTHER DOCUMENTS: (May not be applicable to all applicants)

1. DD Form 214, Certificate of Release or Discharge from Active Duty (for those claiming 5-point veterans' preference eligibility).
2. SF-15 and other substantiating documentation (for those claiming 10-point veterans' preference eligibility).
3. Evidence of National Guard or Reserve Unit member.

Do NOT attach:

Copies of degrees
Copies of certificates
Commemorative memorabilia
Compositions
Publications
Personally Identifiable Media (Driver's License, Social Security Cards, Military IDs, etc.)

Name	Description	Type	Actions

Comments and Certification Information

APPLICANT CERTIFICATION

I certify that, to the best of my knowledge and belief, all of the information on and submitted in support of my application is true, correct, complete and made in good faith. I understand that false or fraudulent information on or attached to this application may be grounds for not hiring me or firing me after I begin work, and may be punishable by fine or imprisonment. I understand that any information I give may be investigated.

☑ I certify that I have read and understand the applicant certification statement provided above.

ADDITIONAL COMMENTS

These materials are copyrighted by Avue Technologies Corporation and may not be extracted, copied, reproduced, displayed to others, or distributed in any form without the prior written consent of Avue Technologies Corporation.
©Avue Technologies Corporation, 2022, All Rights Reserved