Application Walk-Through

Introduction

The DoD CySP application is long and requires careful consideration. The following document has screenshots of each of the pages.

The scholarship is divided into 2 parts. Part 1 determines eligibility. Part 2 requires multiple applicant entries.

The scholarship requires additional documentation, specifically:

- Transcripts (Official or Unofficial)
- Letters of Recommendation
REQUIREMENTS SPECIFIC TO WGU

There are few application requirements that must be answered in a way particular to WGU.

1. All information required to apply is found on the WGU website FAQ at https://www.wgu.edu/lp/it/wgu/cyber-scholarship-program.html# You do not need to check with the Point of Contact to apply. There is no WGU “Augmented Application Package” required.

2. There are particular entries for the GPA requirements for WGU’s competency-based program. Please follow the directions for that section below.

3. You need to upload 3 documents for transcripts.
   a. Academic Transcript
   b. Records of Achievement Transcript
   c. “WGU Statement on Competency-based Education for the DoD CySP Scholarship” (retrieved from WGU website FAQ)

4. You must have at least 24 CUs and 1 Academic year (2 WGU terms) by August 31, 2024 to apply. There are specific instructions for determining your graduation date and when the scholarship begins to apply. Follow the instructions below.

5. You must provide 2 letters of reference. You will upload one file from one recommender. The 2nd letter must be sent from the email address of the recommender. You will provide the relevant information to the scholarship office via this application of the 2nd recommender so that they can match the letter with your application. Please see the WGU website FAQ and the application for guidance on how to select Recommenders.
Account Login

You can apply at this site. Create a new login.

https://www.avuedigitalservices.com/casting/aiportal/control/doLogout
New User Registration

Standard registration. Use your WGU Address.
Home Page

This page will show your active applications and status. If you are a new user, then click “Start Application.”
Introductions and Acknowledgements

This page requires you to accept the terms and conditions of the scholarship. If you cannot agree to the terms, there will be text to tell you that you are not eligible to apply.

Note: You do not need to check with the identified Point of Contact to apply. There is no additional “Augmented Application Package.”
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 1410-1412, 10 U.S.C. §2200, Executive Order 13111, Executive Order 11348, as amended, and DoD Directive 5200.2, DoD’s Blanket Routine Uses (found at Appendix C of 32 CFR Part 310) and the specific uses found in GENSA27 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, Directorate Division at OSU Cybersecurity/Workforce-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 the 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 suitability. 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. ☐

☐ I should 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, meals plan, supplies, transportation, and other miscellaneous academic fee/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. ☐

☐ I should 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: Albert
  Middle Name: 
  Last Name: Einstein

* Current Address: 123 N 
  City: 
  State/Province: Other(Enter below) 
  Other State (if applicable): UT 
  Country: United States of America 
  ZIP/Postal Code: 84025

* Cell Phone: 
  Secondary Phone: 

* Email Address: 
  Confirm Email Address: 

* Mailing Address: 
  * City: 
  * State/Province: 
  Other State: 
  * Country: 
  * Zip/Postal Code: 
  * Student School Email Address: 

Submit Part One

Save and Continue
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 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

Disabilities
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
- Congenital Disorders
- Deafness
- Distortion of Limb or Spine
- Mental Illness
- Mental Retardation
- Missing Extremities
- Complete Paralysis
- Partial Paralysis
- My disability is not one of those listed
- I do not have a disability
- Decline to answer
General Requirements

This page requires you meet the general requirements. If you cannot meet terms, there will be text to tell you that you are not eligible to apply.

Note: For male applicants, you will need to obtain your Selective Service registration #.

The Pathfinders program is an “Are you interested” question. Please select your interest.
Pathfinders Program: Possible Summer 2024 6-Week Internship

* The DoD CySP is partnering with DoD’s Director of Operational Test and Evaluation to offer newly selected DoD CySP Scholars the opportunity to participate in the Test & Evaluation Pathfinders program. The Pathfinders program is a 6-week summer internship (June-July 2024) that provides structured, field-specific training industry professional certifications and processed for adjudicated government security clearance during the summer. The internship is held in a partner training location. All travel is paid to and from the training location, including lodging. Pathfinder Interns will be paid and receive Red Team-specific training/Certification exams, that will include Security+, or Certified Ethical Hacker boot camp style training, hands-on Hack-the-Box security tools, tours of DoD and Federal agencies located near the training location, and access to senior DoD cyber leadership. There is a competitive selection process and selection will be based from the scholar’s interest in the Pathfinder program and submission of information provided to DoD CySP. Course and activity offerings may change due to schedules and availability.

☐ Yes
☐ No
Academic Requirements

WGU is a National Centers of Academic Excellence in Cybersecurity (NCAE-C) academic institution. Select “Yes”

Use the “Select Location” button to find WGU. Click on Utah. Click “Western Governors University,” select “Add” and click “Ok.”

GPA Requirements:

For the question “My GPA is one of the following (no rounding):” select “Yes”

According to WGU’s policy, a “Pass” refers “to a B or better.” On Academic transcripts, the following is stated:

The Academic Transcript’s key states, "Western Governors University and its state affiliates do not calculate a grade point average (GPA) or class rank." The Record of Achievement Transcript contains the statement in the transcript header, “GPA: This student completed each of the listed courses with a GPA between 3.0 and 4.0 on a 4.0-scale." ([https://cm.wgu.edu/t5/WGU-Student-Policy-Handbook/WGU-Transcript-Requests/ta-p/359](https://cm.wgu.edu/t5/WGU-Student-Policy-Handbook/WGU-Transcript-Requests/ta-p/359))
For purposes of this scholarship, WGU encourages students with a sufficient CU count to affirm that their respective “Passes” are a 3.2 or higher for undergraduate or 3.5 or higher for Graduate students.

For purposes of the application, mark the School Grading Scale as “4.0 to 0.0.”

Mark your GPA as 3.5 for both Undergraduate and Graduate students.
Transcripts:

You will need to upload 3 documents in this area. Upload them one at a time and click “Save and Continue” between uploads.”

Please provide both the Academic Transcript and the Records of Achievement Transcript as part of your scholarship submission. They can be either Unofficial or Official.

WGU offers two types of transcripts: an Academic Transcript and a Records of Achievement Transcript. Each contain different information about your student journey. An Academic Transcript will speak to your progress through each term. A Records of Achievement transcript contains the certification of GPA with the following statement “GPA: This student completed each of the listed courses with a GPA between 3.0 and 4.0 on a 4.0-scale.”

In addition to the Transcripts, please add the “WGU Statement on Competency-based Education for the DoD CySP Scholarship” found on the FAQ website.
Example of multiple documents:

**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 must 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.
- All transcripts must be uploaded with the application. Please do not send transcripts directly to the DoD CySP Program Office. Applications submitted without transcripts will be deemed incomplete and not considered.
- **FAILURE TO ATTACH A READABLE SCHOOL-GENERATED TRANSCRIPT WILL RESULT IN DISQUALIFICATION.**

---

Choose File

No file chosen

**Document Uploaded:** Screenshot 2023-08-07 at 10.19.51 AM.png  X

**Document Uploaded:** Screenshot 2023-08-07 at 9.33.07 AM.png  X

---

Save and Continue
Academic Requirements

You must have at least 24 CUs remaining by August 2024 to be eligible for this Scholarship. WGU has 6-month terms. Depending on the term start date, your graduation date will be the date of the end of the last term.

These dates represent the required minimum for 1 Academic years’ worth of scholarship. The scholarship is only awarded in 1-year intervals. If your target graduation date is beyond these dates, go ahead and put the date of the end of your last term. If you plan on graduating prior to the first date listed, you are not eligible for the scholarship.

<table>
<thead>
<tr>
<th>WGU Term Start</th>
<th>Graduation Date in Two Terms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sept. 1, 2024</td>
<td>Aug. 31, 2025</td>
</tr>
<tr>
<td>Oct. 1, 2024</td>
<td>Sept. 30, 2025</td>
</tr>
<tr>
<td>Nov. 1, 2024</td>
<td>Oct. 31, 2025</td>
</tr>
<tr>
<td>Dec. 1, 2024</td>
<td>Nov. 30, 2025</td>
</tr>
<tr>
<td>Jan. 1, 2024</td>
<td>Dec. 31, 2025</td>
</tr>
<tr>
<td>Feb. 1, 2024</td>
<td>Jan. 31, 2024</td>
</tr>
</tbody>
</table>
Junior Year is 60-89 CUs earned. Senior Year is 90+ CUs earned.
* Credits Earned to Date for Declared Major: 60

* Credits Needed to Graduate for Declared Major: 122

* In the FALL of academic year 2024-2025, 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 2024-2025.
  
  Community College
  
  Bachelor’s
  
  Master’s
  
  PhD/Doctorate

Bachelor’s:
  
  Junior Year
  
  Senior Year
  
  Senior Year / 1st Year Master’s

Identify the declared major for the degree level/program you are requesting to be supported by the DoD CySP if selected:

* Declared Major: Cyber Security and Info

* My degree program is: (select one) Online
Congratulations! You’re off to a great start!

Based on the information that you provided in Part 1, we have determined that you are eligible to continue with the application. You may now continue to Part 2 of the application process.
START OF PART 2

Part 1
- Instructions and Acknowledgements
- Personal Information
- Demographics
- General Requirements
- Academic Requirements
- Degree-Related Requirements

SUBMIT PART ONE

Part 2
- * Professional Summary
- * Education
- * Cyber Coursework
- * Skill Set / Certifications
- Experience / Work History
- * Key Projects
- * Recognitions, Honors, and Awards
- * References
- * Letters of Reference
- * Competencies
- * Military Service and Veterans
- Agency Preferences
- Cyber Work Roles of Interest
- Languages
- Computer Programming Languages
- * Security Clearance
- Review Supporting Documents
- Review and Print This Application

CERTIFY AND SUBMIT
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. (200 characters maximum)

Save and Continue
### Education

#### DoD Cyber Scholarship Program

**Instructions**
Please provide details about your education. Once you have added the information you wish to include, click "Continue" to advance to the next section.

#### Details About My Education

<table>
<thead>
<tr>
<th>School Name</th>
<th>City/ State</th>
<th>Degree</th>
<th>Degree Field</th>
<th>Majors</th>
<th>Date Received</th>
<th>Action</th>
</tr>
</thead>
</table>

**Part 1**
- Instructions and Acknowledgements
- Personal Information
- Demographics
- General Requirements
- Academic Requirements
- Degree-Related Requirements

**Part 2**
- Professional Summary
  - * Education
  - * Cyber Coursework
  - * Skill Set / Certifications
  - Experience / Work History
  - * Key Projects
  - * Recognitions, Honors, and Awards
  - * References
  - * Letters of Reference
  - * Competencies
  - * Military Service and Veterans
  - Agency Preferences
  - Cyber Work Roles of Interest
  - Languages
  - Computer Programming Languages
  - * Security Clearance
  - Review Supporting Documents
  - Review and Print This Application

**SUMMIT PART ONE**

**CERTIFY AND SUBMIT**

---

22
Cyber Coursework

List the names of courses you have completed or will complete by August 2024
Skill Set / Certifications

In this section, you are asked to provide information about your technical proficiency and certifications.

Technical Proficiencies
* List technical proficiency, including platforms, networks, languages, and tools used in your past positions. (2000 characters maximum)

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)
- GISP - Certified Information Systems Security Professional ([ISC]2)
- GISP Associate - Certified Information Systems Security Professional Associate ([ISC]2)
- Cloud+ - CompTIA Cloud+ Certification
- GND - 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
- GOFE - GIAC Certified Forensic Examiner
- GCIA - GIAC Certified Intrusion Analyst
- GCHH - GIAC Certified Incident Handler
- GIISP - Global Industrial Cyber Security Professional
- GSSEC - GIAC Security Essentials Certification
- GSSL - GIAC Security Leadership Certification
- GSNA - GIAC Systems and Network Auditor
- Network+ - Network+ (CompTIA)
- PenTest+ - CompTIA PenTest+
- SCYBER - Cybersecurity Specialty Certification (Citco)
- 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
☐ CBP - 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]
☐ CSCE - Certified Security Computer User [EC-Council]
☐ CSTA - Certified Security Testing Associate
☐ CVP - Certified Virtualization Professional
☐ ECII - EC-Council Certified Incident Handler
☐ ECSR - EC-Council Certified Security Analyst
☐ ECSP Java - EC-Council Certified Secure Programmer Java
☐ 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
☐ GISIP - GIAC Information Security Professional
☐ GLE - GIAC Law of Data Security & Investigations
☐ GMOB - GIAC Mobile Device Security Analyst
☐ GMON - GIAC Continuous Monitoring Certification
☐ GNFA - GIAC Network Forensic Analyst
☐ GOS - GIAC Open Source Intelligence
☐ GPRE - GIAC Penetration Tester
☐ GPFA - GIAC Certified Perimeter Protection Analyst
GPPA - GIAC Certified Perimeter Protection Analyst
GPCY - 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
GSPP.NET - GIAC Secure Software Programmer-.NET
GSPP-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
HC/ISSP - 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
MNAD - 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

If you have not entered any work history previously, there will not be any entries shown below. For any work history you have, you must provide information here. Click Add a Federal Position to add entries for Federal positions. Click Add a Military Position to add Military positions. Click Add a Non-Federal Position to add a private sector position. If you do not have work history to add, you may leave this section blank and move on to the next question. When your work history is complete, click Save and Continue.

Add a Federal Position  Add a Military Position  Add a Non-Federal Position

UPDATE CAREER PORTFOLIO

Save and Continue
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. (2000 characters maximum)

* 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: (1000 characters maximum)

Describe any academic recognition (certifications included), honors, distinctions, or awards that you have received. This is very important, as it counts towards the evaluation criteria.

NOTE: The recognition, honors, distinctions, or awards that you describe in this supplemental statement need not be job-related.

Be sure that you include any scholarships, membership in any honorary societies to which you were admitted because of academic accomplishment, and any significant leadership roles in academic groups, organizations, societies, or associations to which you were nominated or elected.

Provide sufficient summary information for evaluators to understand the period or date of the accomplishment, the awarding institution or organization, and what you did to earn the recognition.

Save and Continue
References

Instructions

Please provide references by clicking the "Add a Reference" button. You may edit or remove an individual entry by selecting the corresponding link.

Note:
Individuals listed to provide references in this section should be different than the individuals you have chosen to provide you with a letter of reference.
Letters of Reference

You must provide 2 letters of reference. You will upload one file from one recommender. The 2nd letter must be sent from the email address of the recommender. You will provide the relevant information to the scholarship office via this application of the 2nd recommender so that they can match the letter with your application.
Competencies

This is a short response/essay portion.

Describe your knowledge and ability in each of the six (6) competency areas below. The evaluation points are very high in this area. You must address each area identified. If you do not provide this information, your package will be deemed non-responsive and will not be considered.

* 1. Knowledge of the techniques of the cybersecurity discipline, including encryption, access control, physical security, training, threat analysis, and authentication. (2000 characters maximum)

* 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. (2000 characters maximum)

* 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. (2000 characters maximum)

* 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. (2000 characters maximum)

* 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. (2000 characters maximum)

* 6. Ability to express facts and ideas in writing in clear, convincing, and organized manners appropriate to the audience and occasion. (2000 characters maximum)
Military Service and Veterans

You may be asked to provide additional documentation depending on your answer.
Agency Preference

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

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 (USSTRATCOMC4)
- United States Africa Command (USAFRICOM)
- United States Cyber Command J5 (USCYBERCOM J5)
- United States Cyber Command J7 (USCYBERCOM J7)
- United States Special Operations Command

Department of the Air Force (AF)
- AF CYBERCOM
- 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 HODA CIO O-6 (DCSG-6)
- U.S. Army Network Enterprise Technology Command
- U.S. Army Redstone Arsenal (US Army TSMO)

Department of the Navy (NV)
- Commander, Naval Air Systems Command (COMNAVAIRSYSCOM)
- Naval CYBERCOM (FLT CYBER)
- 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 (NAWOCWD)
- Naval Air Warfare Center Weapons Division (NAWOCWD) 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 (COMNAV/SEASYSCOM)
- 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 (NAVSURFWRCCEN)
- Naval Surface Warfare Center Dahlgren Division (NSWCD)
- Naval Surfaces Warfare Center, Crane Division (NSWCCD)
- Naval Surfaces 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 (MC COG)
- Marine Corps Systems Command (MCARCSYSCOM)
- 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)
- Counterintelligence Analyst (121)
- Exploitation Analyst (121)
- Target Developer (131)
- Target Network Analyst (132)
- Target Reporter (134)
- Warning Analyst (141)
- Multi-Disciplined Language Analyst (151)

**Investigate - Work Roles**
- Forensic Analyst (211)
- Cyber Crime Investigator (221)
- Cyber Defense Forensics Analyst (231)

**Collect and Operate - Work Roles**
- All-Source Collection Manager (311)
- All-Source Collection Requirements Manager (312)
- Cyber Operator (321)
- Access Network Operator (321)
- Interception 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)

**Security Promotion - Work Roles**
- Authorizing Official (611)
- Security Control Assessor (612)
- Software Developer (621)
- Security Software Assurance (623)
- Information Systems Security Developer (631)
- Systems Security Developer (632)
- Systems Requirements Planner (641)
- Enterprise Architect (651)
- Security Architect (661)
- 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)
- CYBERSEC Manager (723)
- Cyber Legal Advisor (731)
- Privacy Compliance Manager (732)
- Cyber Workforce Development and Manager (751)
- Cyber Policy and Strategy Planner (752)
- Program Manager (801)
- IT Project Manager (802)
- Cyber Support Manager (803)
- IT Investment/Portfolio Manager (804)
- IT Program Auditor (805)

Certify and Submit
### 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.

<table>
<thead>
<tr>
<th>Language</th>
<th>Oral Proficiency</th>
<th>Written Proficiency</th>
<th>Listen Proficiency</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Add

Save and Continue
Programming Languages

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**: 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

Save and Continue
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 (SC/CI/14)
- Q (Atomic Energy Act)
- Other
- Not Applicable; I have not held a U.S. Government-issued security clearance

Save and Continue
Instructions

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. 3. Evidence of National Guard or Reserve Unit member.

OTHER DOCUMENTS: (May not be applicable to all applicants)
1. Transcripts - Official or unofficial. **Optional for Associate Degree applicants only.** 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.

Do NOT attach:
- Copies of degrees
- Copies of certificates
- Commemorative memorabilia
- Compositions
- Personally Identifiable Media (Driver’s License, Social Security Cards, Military IDs, etc.)
Instructions and Acknowledgements Summary

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 106-337). 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). Per the FY23 NDAA, The DoD Cyber Scholarship Program (DoD CySP) will become the DoD Cyber and Digital Service Academy (DCDSA) in next year's cycle.

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).

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) 854-6200 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.