

Opportunity Title: OCIO Cyber Student Intern Program

Opportunity Reference Code: DHS-CSIP-2019

Organization U.S. Department of Homeland Security (DHS)

Reference Code DHS-CSIP-2019

How to Apply A complete application package consists of:

- An application completed in Zintellect
- Academic Transcripts:
 - College students must submit an unofficial transcript. Transcripts must include Fall 2018 grades. If summer courses were taken, transcripts must include these grades. [Click here for detailed information about acceptable transcripts.](#)
 - High School Students may submit a copy of the student academic records printed by the applicant or by academic advisors from internal institution systems. Selected high school students must provide proof of acceptance/enrollment for Fall 2019 upon acceptance of an appointment.
- A current résumé/CV

If you have questions, send an email to SciEdPrograms@orau.org. Please include the reference code for this opportunity in your email.

Detailed information about the program can be found at:

<https://www.dhs.gov/homeland-security-careers/cyber-student-intern-program>

Application Deadline 4/18/2019 11:59:00 PM Eastern Time Zone

Description Those selected for the Secretary's Honors Program Cyber Student Intern Program (CSIP) in the [Office of the Chief Information Officer \(OCIO\)](#) will have an opportunity to experience and learn about the cybersecurity work completed every day by dedicated DHS personnel. Each assignment is unique, providing Selectees the opportunity to be involved in one or more important projects.

OCIO Student assignments include:

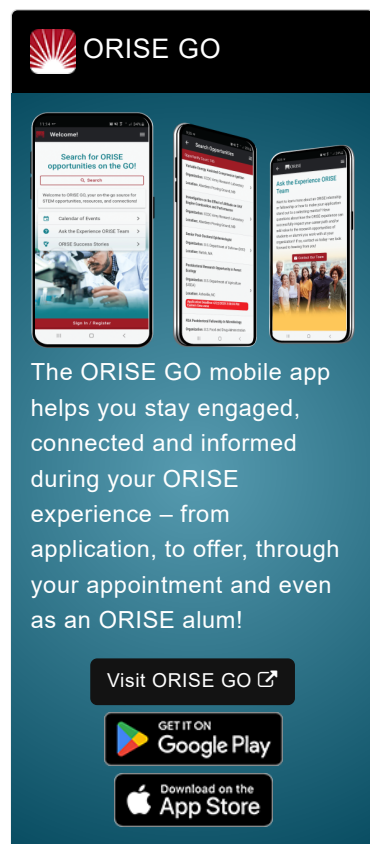
Office of the Chief Information Security Officer

Students will engage with and develop an understanding of DHS cyber efforts in the following areas:

- Federal Information Security Management Act (FISMA) Compliance and Technology
- Cyber Threat
- DHS Cybersecurity Policy & Remediation
- Program Management
- National Security Systems Risk Governance, Architecture, Supply Chain Risk Management (SCRM)
- Security Architecture and Engineering

Office of the Chief Technology Officer, or Information Technology Services Office

- Learn and develop skills in information technology to include agile, cloud computing, digital transformation, IT modernization, cryptography, cybersecurity and DevSecOps for DHS initiatives.



Opportunity Title: OCIO Cyber Student Intern Program

Opportunity Reference Code: DHS-CSIP-2019

- Develop skills to communicate with IT professionals who specialize in Systems Architecture, Enterprise Architecture, Data Management, Cloud Computing and Software Development.
- Learn to perform system backup and maintenance functions.
- Participate with DHS personnel on special projects as determined by the Solution Architecture staff.
- Learn needs analysis for projects in research for solutions for identified needs.
- Participate in projects related to developing and updating user and technical documentation to increase this skill set.
- Create and publish interactive reports and white papers under the direction and guidance of DHS personnel.
- Participate with DHS personnel in maintaining, developing, designing and updating OCTO Atlassian Suite in order to learn or increase this skill set.
- Gain hands-on, practical experience with the full gamut of technology, roles, and responsibilities of the professionals at DHS.

Appointment Length

This appointment is for a summer placement of up to 10 weeks.

Participant Benefits

- A stipend is available for qualified students.
- Qualified students will be offered a Housing Allowance.
- No Relocation will be paid.

Location

Students will be assigned to the Office of the Chief Information Officer, Headquarters, located at 301 7th Street S.W., Washington, DC 20024.

Nature of Appointment

The participant will not enter into an employee/employer relationship with ORISE, ORAU, DHS, or any other office or agency. Instead, the participant will be affiliated with ORISE for the administration of the appointment through the ORISE *Letter of Appointment* and *Terms of Appointment*.

While the participant will not enter into an employment relationship with DHS or any other agency, this opportunity will require a suitability investigation/background investigation. All placements are contingent upon successful completion of the background investigation process and subsequent ability to gain access to the assigned facility. The anticipated background investigation requirements for students participating at OCIO is: Public Trust or Secret.

Qualifications Applicants must:

- Meet one of the following conditions:
 - Be currently enrolled at least half-time in pursuit of an Associates, Bachelors, or Masters degree at an accredited college or university, majoring in 1) Science, Technology, Engineering, or Mathematics (STEM); or 2) Cybersecurity Operations / Cybersecurity Defense;

Opportunity Title: OCIO Cyber Student Intern Program






Opportunity Reference Code: DHS-CSIP-2019

and/or 3) a desire to work in field of cybersecurity upon graduation.
Students who graduate (Associates or Bachelors degrees) in spring 2019 must provide proof of acceptance or enrollment in a Bachelors or Masters degree program for Fall 2019 to be eligible for participation; OR

- Be enrolled as a high school senior expected to graduate by Summer 2019 and planning to be enrolled in an Associates or Bachelors program for the Fall 2019 semester.
- Have a minimum acceptable GPA of 3.0 on a 4.0 scale as indicated on most recent transcript. A legible copy of most recent transcript (official or unofficial) must be provided to verify education enrollment and GPA.

OCIO is especially interested in applicants that have completed coursework or previous experience related to:

- Threat analysis;
- Risk assessment;
- Incident response;
- Security architecture and engineering;
- Network monitoring/network defense;
- Cybersecurity research and technical writing;
- Basic knowledge and understanding of industry best practices regarding policies, governance, strategies and standards in cybersecurity;
- National Security Systems governance and Supply Chain Risk Management (SCRM); and,
- Testing and development.

- Eligibility Requirements**
- **Citizenship:** U.S. Citizen Only
 - **Degree:** Currently pursuing a High School Diploma/GED, Associate's Degree, Bachelor's Degree, or Master's Degree.
 - **Overall GPA:** 3.00
 - **Discipline(s):**
 - **Computer, Information, and Data Sciences** ([16](#) )
 - **Engineering** ([2](#) )
 - **Mathematics and Statistics** ([10](#) )
 - **Other Non-Science & Engineering** ([1](#) )
 - **Social and Behavioral Sciences** ([3](#) )
 - **Age:** Must be 16 years old by 4/18/2019

Affirmation I certify that I am a U.S. citizen who is at least 16 years of age at the date of this application, and am a graduating high school senior, **or** am enrolled at least part-time in a degree seeking program in pursuit of an Associate's, Bachelor's, or Master's degree at an accredited college or university with:

1. A major in one of the eligible fields noted above;
2. An interest in working in the field cybersecurity upon graduation;
3. A cumulative grade point average (GPA) of 3.0 on a 4.0 scale;
4. A projected college graduation date of December 2019, or later.