The GW CyberCorps Program

www.seas.gwu.edu/cybercorps

Introduction

The need for educated personnel in the government's cyber security workforce is critical to the nation's security. As evidenced by remarks of President Obama in his landmark speech of May 29, 2009 and cyber security legislation in the current Congress, time is of the essence in meeting this need. The federal government's most successful, but still limited, pipeline for young cyber security talent is the CyberCorps program of the federal government. One of the most successful feeder institutions into this pipeline, educating and sending computer security experts into government service since 2003, is The George Washington University's Partnership in Securing Cyberspace through Education and Service (Project PISCES). This program has produced 106 federal government employees to date, and 11 more scholars are on track to graduate by 2021.

The George Washington University (GW) is a designated Center of Academic Excellence in Information Assurance Education and Research (CAE/IAE and CAE/IAE-R), designated by the National Security Agency (NSA) in cooperation with the Department of Homeland Security (DHS). GW provides CSIA education opportunities for students with diverse backgrounds to become cybersecurity professionals and help protect the safety and security of our nation's information infrastructure. It does this by combining scholarships, university courses in computer security and information assurance, internships, laboratories, and government service, with a unifying and reinforcing Seminar that prepares students with the knowledge, perspective, and expertise to perform competently in their future government positions, repay the federal government its hefty investments in their education, and serve their country.

The GW CyberCorps is a group of scholarship students supported by the Scholarships for Service (SFS) program of the National Science Foundation and the Cybersecurity Scholarship Program (CySP) supported by the Department of Defense. Both of these are also supported by the Department of Homeland Security. Our multidisciplinary academic program in information assurance, our signature government guest lecturer Seminar, and our location at the center of the government cyber security workforce make this effort attractive for students and the government, and our placement rate of more than 95% for CyberCorps graduates reflects that.

GW CyberCorps Objectives

Our current CyberCorps program has six objectives:

1. *Produce graduates with knowledge of cybersecurity issues and mechanisms and the technical expertise to design and build secure information systems in the future.* Our graduates have completed at least 24 hours of cybersecurity course work including 12 hours of GW's signature "Seminar" course.

2. *Provide graduates with a global societal and ethical context within which to apply their technical expertise.* The required "Seminar", a course that runs throughout the scholars' two-year program, includes speakers on issues such as privacy, intellectual property, computer crime, and information warfare, and provides numerous opportunities to engage the speakers in informal discussions of the efficacy of the technological armada of security and information assurance tools utilized in response to these issues.
3. *Provide graduates with practical experience working within the culture of the federal government.* All students who have graduated from the program to date also participated, during the summer, in paid internships at federal government agencies, national laboratories, or Federally Funded Research and Development Centers.
4. *Provide graduates with opportunities to develop and demonstrate their ability to write and speak for both technical and non-technical audiences.* During weekly "Seminar" meetings, students present "News of the Week in Cybersecurity" to their peers, visiting speakers, and course instructors. Students also prepare written system security plans for their instructor and present these to their peers.
5. *Expand the educational opportunities for US citizens who are traditionally underrepresented populations in the computer field.* By July 2021, 38% of our graduates were women and 52% were from underrepresented groups.
6. *Establish a peer and near-peer mentoring network among prospective students, current students and students who have already completed the program and gone on to work for the federal government.* We have found that an informal network starting with assignment of "buddies" to first-year CyberCorps students and including our SFS and CySP alumni has been most effective in mentoring students in the program and placing them in jobs when they graduate.

Academic Program for CyberCorps Students

GW students pursue a well-defined degree in a major that incorporates some aspect(s) of computer security and information assurance. They must take a minimum number of cybersecurity-related courses in their home department beyond the courses required for their degree. They may also be required to take additional cybersecurity courses outside of their department that are appropriate for their major.

Our CyberCorps students have received degrees in computer science, electrical engineering, engineering management and systems engineering, business administration, public policy, forensic sciences, and information technology. The structure of our program is flexible and allows students from other fields as well to have a strong minor in cybersecurity. Seven GW departments have formal programs defined that satisfy both the department degree requirements and our cybersecurity requirements. We welcome other departments at GW to increase this number.

After completing certain cybersecurity coursework, students are eligible to apply for one or more National Training Standard certifications. These certifications are useful to some government employers and qualify students who choose to work for some federal agencies for higher rates of pay. GW has been accredited to award these certifications and our graduates receive them once they have completed the appropriate coursework and administratively applied for them.

Signature Seminar: Taking Advantage of Our Location in the Nation's Capital

GW requires all cybersecurity scholarship students to complete Computer Science 6534, Cybersecurity and Governance for all four semesters of their scholarship programs. CSci 6534 is GW's distinctive course that underlies its success in educating and placing CyberCorps graduates in federal agencies. Students' participation in this course begins the process of building working relationships that become a very important success factor in their future careers. It is the unifying and reinforcing experience that prepares students with the knowledge, perspective, and expertise to perform competently in their future government positions, repay the federal government its hefty investments in their education, and serve their country.

At a dedicated weekly time during both academic years of the program, for a full twelve credit hours of instruction, it brings cybersecurity students together and guides them through a curriculum designed to give them a thorough understanding of the roles and responsibilities of the Federal Government in Cyber Security, an overview of the technical aspects of Cyber Security, and familiarity with the Federal Information Security Management Act (FISMA) and with cyber legislation currently proposed and under discussion. Over the two-year period, the course essentially grooms GW's CyberCorps students to succeed by developing their technical, analytical, managerial, presentation, and writing skills with regard to cybersecurity issues. It provides a baseline of common knowledge of relevant federal policies and mandates and an informed picture of federal government roles, responsibilities, and processes. It reviews basics of U.S. Constitution and law and steeps students in the cybersecurity elements necessary to planning federal computer systems within a framework that is cognizant of privacy, cost, risk, civil liberties, and public acceptance.

The students study current federal civilian and Defense Department policy and compliance programs by examining the FISMA process and the related set of security controls. They engage in the entire Security Certification and Accreditation, audit, and System Security Plan processes. The course readies students to contribute to a government cybersecurity environment on their first day in the federal workforce.

The course begins each fall with second-year students presenting their federal agency summer internship experiences to the cohort of their peers and new first year cybersecurity students. With input from both faculty and second-year students, first-year students prepare resumes, develop and refine interview skills, and discuss how their background, education and experience will contribute to their success in the federal workplace. The opportunity to videotape practice interviews and review the results is provided.

Ongoing topics of discussion include threats, attacks, and vulnerabilities as well as mechanisms for mitigation, detection, and reconstitution of systems. Students are constantly called on and engaged to consider these matters. In the laboratory, students have hands-on opportunities to develop System Security Plans incorporating Plans of Action and Milestones to secure the lab system. They practice making workstations Federal Desktop Core Configuration compliant and hardening all servers to the DoD Gold Disk standard. They follow this by performing audit, Certification and Accreditation for each system. Each week, the instructor assigns students to discuss a current attack affecting Federal systems. In examining each attack, students study the system vulnerabilities, effective mitigation strategies that are both technical, policy-oriented, and correspond to the FISMA controls that would have prevented the

attack. These student presentations lead to lively and informative discussions among the students, instructor, and guest lecturers who are able to add key insights, knowledge and observations. In addition, the process effectively builds esprit de corps and public speaking skills, both essential to the development of these future government cadres.

More experienced students develop a System Security Plan for a fictitious Government system that is iteratively critiqued and refined through interaction of both the instructor and student. By the end of students' two years of participation in the course, they are well-versed in the use of government processes to analyze computer systems, perform risk assessments and document systems' FISMA compliance. As a result of these exercises, one student reported a sense of "standing out from the veteran employees" and subsequently received a job offer during his summer internship. Almost every week, a government official or industry expert speaks, reinforcing concepts, sharing insights, and meeting informally with scholarship students. The field is fast moving and in response, we frequently update Seminar topics, exam questions and answers in technology, law, and government policy. The following represents a small sample of the questions, terms, and readings on which we recently tested students:

- Who is in charge of Cyber for the Federal Civil Executive Branch?
- Why is monitoring the Departments and Agencies different from monitoring the DoD?
- What laws apply on the Internet?
- Who are the Federal CTO and the Federal CIO?
- Where by authority can the NSA monitor? The CIA? The FBI? US-CERT? Departments and Agencies? Private Sector?
- Who must report their computer incidents to US-CERT?
- What law prevents monitoring of private citizens in the US without a warrant or permission?
- When does Microsoft release their patches?
- Name all of the speakers from this semester and give a short description of their roles in the industry.
- Define and explain these terms at an overall level: CIP, ISAC, PII, C&A, HSPD-54, IV&V
- What are these and what is their importance and relationship to CSIA:
  - Federal Information Security Management Act
  - President's Management Agenda
  - National Information Assurance, Certification and Accreditation Process
- Explain the main ideas in
  - NIST 800-18 Guide for Developing Security Plans for Federal Information Systems
  - NIST 800-30 Risk Management Guide for Information Technology Systems
  - OMB Memorandum 06-19 Reporting Incidents Involving Personally Identifiable Information
  - Incorporating the Cost for Security in Agency Information Technology Investments

- OMB Circular A-130, Appendix III Security of Federal Automated Information Resources, November 2000

Finally, the course provides students valuable informal networking and contacts. Personal interactions with speakers, program alumni, and instructors have led to internships and jobs. Students and graduates establish and rely on these personal and professional friendships and contacts to serve as sounding boards for work-related advice and to provide assistance in their searches for their next positions.

Supporting Laboratories

A number of laboratories are available to students for their security-related experiments. One is a completely stand-alone network that allows research and teaching while not having the possibility to disrupt the campus network or the Internet. There is another computer systems lab at GW used for the Computer Network Defense course as well as for GWU's Collegiate Cyber Defense Competition team (http://www.nationalccdc.org/). There is also a forensic sciences lab with several Windows- and Linux-based forensic and steganography tools. Finally, as part of its participation in CyberWatch (www.CyberWatchcenter.org), GW students may use CyberWatch virtual lab facilities where GUI-interface firewall devices are available to offer challenging security oriented-technical training to managerially-oriented students who are not accustomed to using command line interfaces.

Using Washington as a Classroom

Students also take advantage of our Washington location to visit congressional hearings and other events where they see cybersecurity issues debated and policy formulated. Often, professors asked to speak at these events invite the students along. Typical conferences attended by many students include BlackHat, FOSE, the State of the Net Conference, and recent events sponsored by the WashingtonPostLive (and CSPRI) and the Future of Privacy Forum (and CSPRI). Many have also taken a field trip to the National Cryptologic Museum adjacent to the headquarters of the National Security Agency in nearby Fort Meade, Maryland.

Students visit various conferences that match their security interests. For example, we have had CyberCorps students travel to Crypto, the annual International Cryptography Conference and to the RSA Conference. GW has also had a team of master's and undergraduate students compete at the Mid-Atlantic Regional Competition of the National Collegiate Cyber Defense Competition.

Recruitment, Screening, and Selection Process

Recruitment

Our recruiting and selection processes are in place and refined each year. We reach out to students at the undergraduate and graduate level by informing groups of likely prospects, such as student chapters of the Association for Computing Machinery (ACM), the Institute of Electrical and Electronics Engineers

(IEEE), the High Technology Crime Investigation Association (HTCIA), and the Association of Forensic Science Students (AFSS) with email notices of the scholarship availability. Some of the involved faculty members include a notice about the recruitment for scholarships in their email signature.

Program Information and Targeted Majors

The official website for GW's CyberCorps, www.seas.gwu.edu/cybercorps, is the main source of information for prospective students and employers and is used as a current reference for information about the program by students and faculty alike, including detailed links to descriptions of each academic program GW CyberCorps students are in or have undertaken in the past. We have included written testimonials by former students, success stories from news releases of organizations that have hired former students, scholarship application forms, frequently asked questions about the program, information for prospective government employers, contact information for the program office, and a wealth of practical information for current CyberCorps students.

We make scholarship information available to undergraduate and graduate students from all university disciplines. We attempt especially to reach students in fields where our previous graduates have come from – Cybersecurity in Computer Science, Electrical Engineering, Computer Science, Information Systems, Engineering Management, Business Administration, Forensic Sciences, and Public Policy. We also continuously look for students with good computer skills who are in fields with emerging needs for CSIA specialists, such as health care management and international affairs.

While the majority of our students are in their twenties and in computer science, we do not limit our recruiting to only technical specialists; nor do we recruit only rising juniors or those just graduating with a bachelor's degree. We have also selected applicants who were older or had limited computer science experience but significant potential. Each one has gone on to succeed in their federal careers. One was described in Government Computer News as "the model for a federal scholarship initiative." Recruiting across disciplines, together with the required seminar that provides support, connections, networking, and "insider" information sets us apart, expands the base of prospective students, and serves the students, university, and government well, by creating a learning environment where a heterogeneous cohort learns to work (and sometimes play) together and to appreciate the contributions that persons from various backgrounds and disciplines can make to solving IA problems in the workplace.

Screening

Students apply for the scholarship using an online application (https://cspri.seas.gwu.edu/cybercorps-application). Any questions not answered on the website are referred to a Program Assistant. Any that that person cannot answer, for example technical questions related to specific courses, are referred to the Project Director. We elicit from each applicant their transcripts (and Graduate Record Exam scores, if appropriate). They must also submit two letters of recommendation that describe the applicant's ability to identify, analyze, and solve problems and the applicant's knowledge of information technology and information security. Except in unusual circumstances, at least one letter of recommendation is from a faculty member with recent exposure to the

student in a learning situation. Each student applicant also submits a short written statement of why the student believes that she or he should be selected for a scholarship.

We provide a form for the recommendation letters that, in addition to the general narrative comments, asks the recommender to rate each applicant in the areas of academic merit and professionalism. Specifically, we ask the reviewers to comment on these attributes of the candidates:

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

2. Knowledge of the human factors in information security, 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.

After an initial screening that checks applicant eligibility (U. S. citizen and grade point average at least 3.0, valid transcript submitted), the application is sent on to undergo further scrutiny by a review panel.

Selection

The review panel consists of the co-principal investigators at GW, the seminar instructor, one graduate from the GW CyberCorps program now serving as a federal government employee, and faculty members appropriate to the applicant's proposed major field of study. It first evaluates the applicant's academic performance based on his/her transcript, grade point average, academic honors, and other recognition. It also considers the Graduate Record Exam scores if the applicant is applying for a graduate program. It then develops an overall score for the applicant's two letters of recommendation by combining the narrative evaluation with the academic merit and professionalism ratings provided by the recommenders.

As a final step in the review process, the panel interviews applicants selected from those with the highest scores based on the combination of their total academic score, recommendation letters, and student

statements. (Out-of-area candidates are typically interviewed via Skype, but may be invited to visit at GW's expense if this is deemed warranted.) During the interview, the panel further assesses the applicant's knowledge, abilities, academic merit and professionalism. Each member of the panel awards the applicant an interview score. Finally, the applicant's overall score is computed using the academic score (35%), the two letter-of-recommendation scores (15%), the interview scores (35%), and scores for the applicant's written statement (15%). The highest-ranking applicants are selected for awards based on the amount of funding available.

November 13, 2021