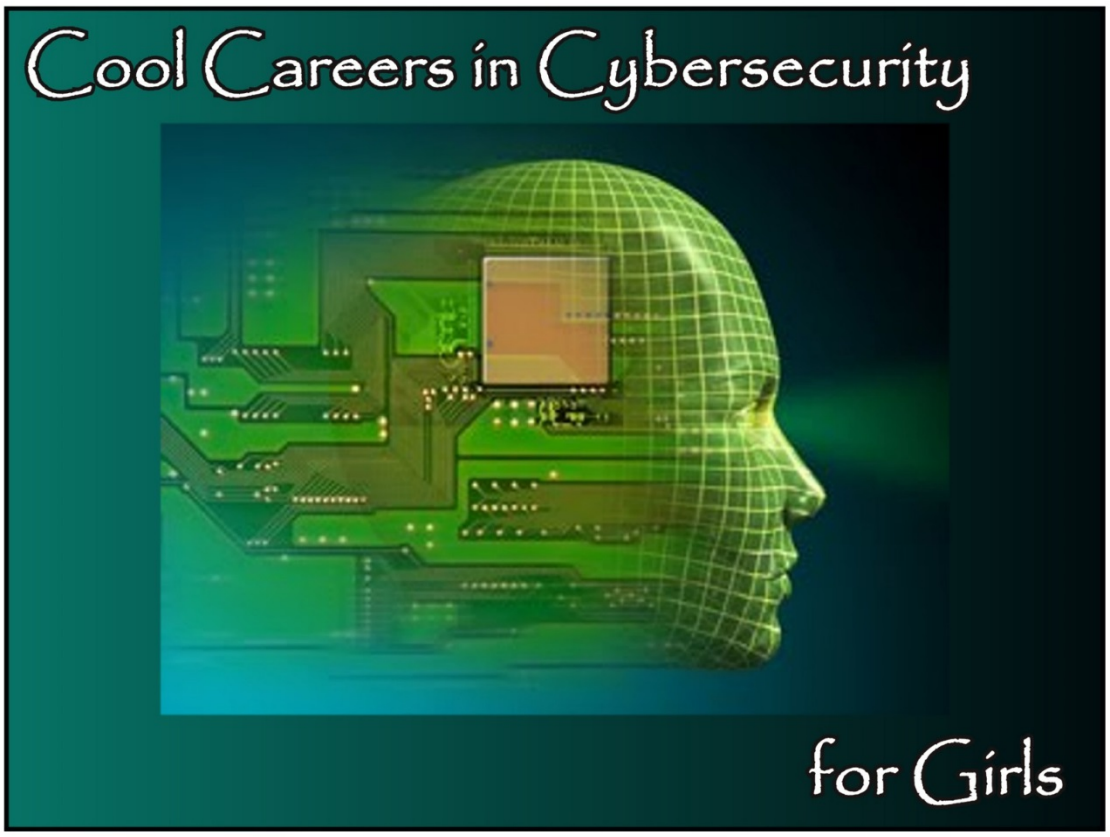
MARYLAND OF OPPORTUNITY. for Cyber

CSM college of southern maryland

Info Security Crime Investigator • Malware Analyst • Incident Responder • Forensic Analyst

Security Architect • Penetration Tester • Network Security Engineer



Vulnerability Researcher • Exploit Developer • Security Auditor

Computer Crime Investigator • Security Operations Center Analyst • Intrusion Analyst

national CyberWatch center K12

ETPRO

NSF

Cool Careers in Cybersecurity for Girls™ Workshop C34G

December 3, 2014
10 a.m. to 1:00 p.m.
Center for Business & Industry at the
College of Southern Maryland – La Plata Campus

Cool Careers in Cybersecurity for Girls (C34G) educates, inspires, and provides girls with the information, skills and resources necessary to navigate the professional pipeline in the vast field of cybersecurity. Our vision is put into action through programs and a focus on cyber stewardship, activities to make a safer and more secure society, by delivering high-quality, innovative activities that inspire girls to pursue careers in cybersecurity.

The National CyberWatch Center K-12 Division, led by Educational Technology Policy, Research and Outreach is excited to partner with the College of Southern Maryland and the Maryland Department of Business and Economic Development to offer another outstanding Cool Careers in Cyber Security for Girls Workshop at the College of Southern Maryland, La Plata Campus. The event would not be possible without women professionals volunteering their time. We would like to thank the women from the following organizations who volunteered their time to help middle school girls understand how their innate gifts and interests can help them have a successful career in any STEM field.

- CyberPoint International
- Integrity Applications Incorporated (IAI)
- MAXIMUS
- Montgomery College
- National Security Agency (NSA)
- Northrop Grumman
- Northrop Grumman WiNGs
- Smartronix, Inc
- Startup Partners, Inc.
- University of Maryland Baltimore County (UMBC)

Thank you once again for your time and commitment to this event.

Presenter Guide

The National CyberWatch Center K-12 Division led by Educational Technology Policy, Research and Outreach, in partnership with the College of Southern Maryland and the Maryland Department of Business and Economic Development thanks you for volunteering to present at the Cool Careers in Cybersecurity for Girls Workshop. We could not do this without your willingness to share your experiences with our middle school girls.

This presenter guide will help you prepare for the day and assist you in answering student questions. It contains:

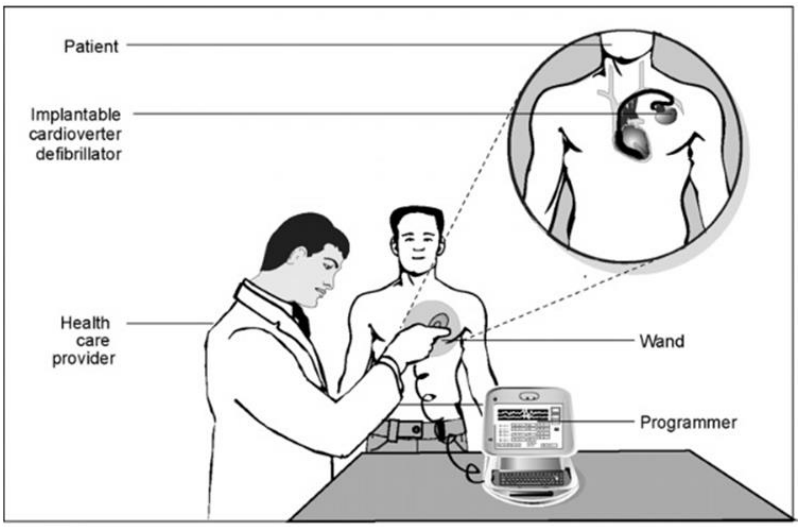
- Scenario
- Agenda
- Annotated Agenda with additional ideas on ways you can help the event go smoothly
- Activities and clues (in case you are curious about the crime)
- Questions students have asked Women STEM Professionals about Cybersecurity in the past
- Directions and parking information

Scenario

Middle school girls become Cyber Super-Investigators (CSI) for a day to solve a cyber-crime.

During this interactive crime solving event, girls learn from women in diverse companies and agencies about what it takes to navigate the professional pipeline in the vast fields of Cybersecurity and Information Assurance, as well as other science, technology, engineering, and mathematics (STEM) fields.

The middle school girls complete hands-on activities with guidance from cybersecurity and STEM professionals in order to gather clues to help solve the crime. This year's cybercrime scenario focuses on vulnerabilities in networked medical equipment.



Source: GAO.

On an episode of the *Showtime* series *Homeland,* Vice President Walden's pacemaker was hacked becoming the weapon for his assassination. In a *60 Minutes* interview with former Vice President Dick Cheney, he confirmed that the possibility of his pacemaker being hacked had been discussed and the device's wireless access had been disabled to prevent such an attack on his life.

Although it may sound like science fiction several studies have proven that flaws in cyber security of medical devices could be exploited to induce death.

- Computer scientist Kevin Fu has demonstrated in a research lab that he could hack into a combination heart defibrillator and pacemaker to induce potentially fatal electric jolts.
- Researchers at computer security firm McAfee share they have found a way to hack into an insulin pump to make it release multiple days' worth of insulin.
- Security analysts Terry McCorkle and Billy Rios discovered a simple password vulnerability affecting over 300 devices including ventilators, drug infusion pumps, external defibrillators, patient monitors, and laboratory and analysis equipment. Devices could be exploited to change critical settings or modify the device.

In the case of our scenario, the 2014 Cool Careers Cyber Crime: *Networked Medical Equipment Vulnerabilities*, the all girls' middle school Cyber Super-Investigators (CSI) have been hired to examine in greater detail how medical devices could be breached and make recommendations to the U.S. Food and Drug Administration.

The girls will collect and explore a variety of digital and physical evidence to learn more about medical device vulnerabilities. Clues provided by the lead investigators, the cyber professionals speaking at the Cool Careers in Cybersecurity for Girls Workshop, will help the middle school girls in their investigation!

Related Content

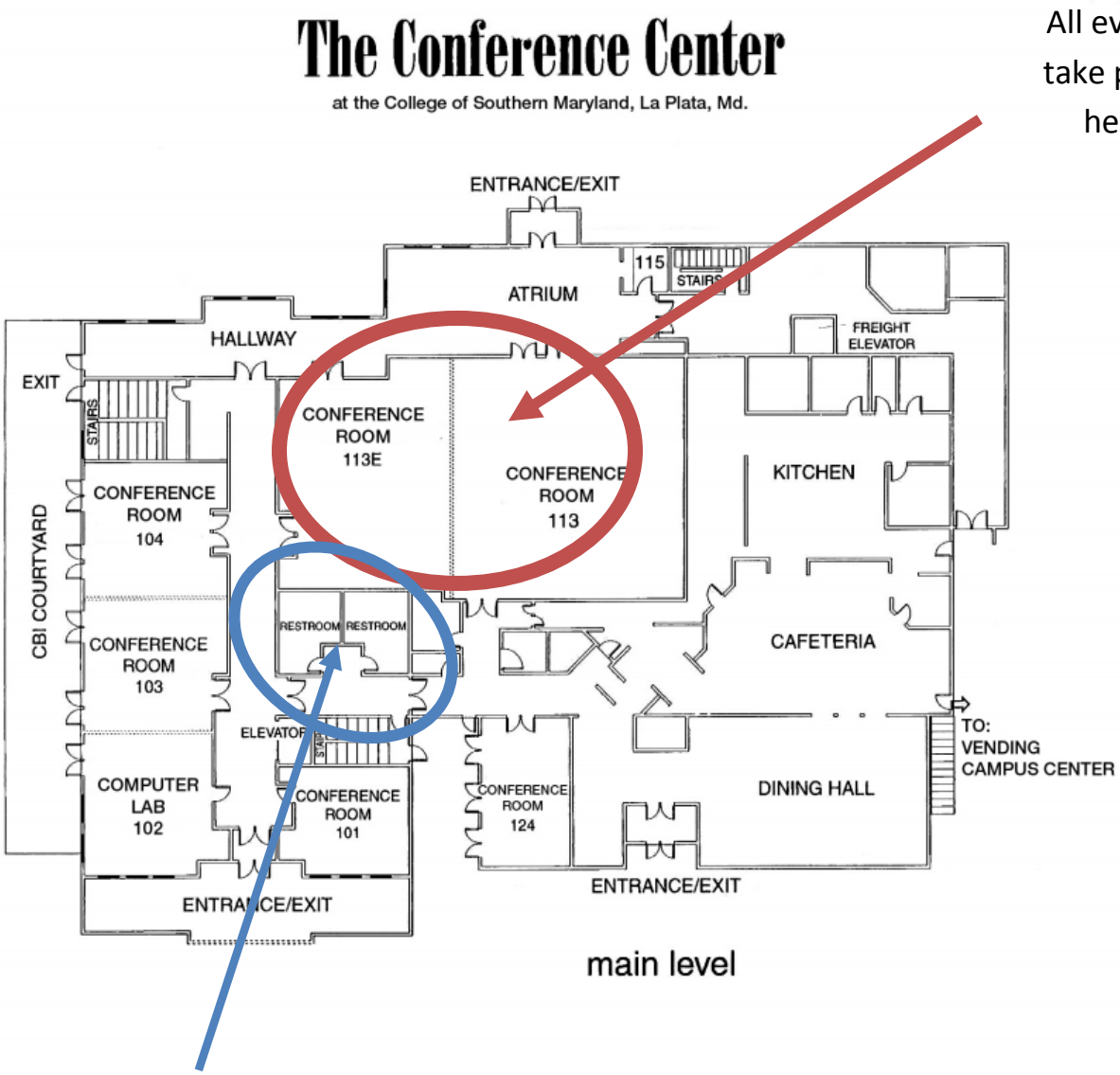
Some of the reports indicate some rudimentary causes for medical equipment breaches; some from known software flaws, and others from end-user related vulnerabilities including:

- Lack of authentication to access or manipulate the equipment
    - Table activity: Physical security and lock picking
    - Table activity: Find the USB drives
- Weak passwords set by users as well as weak or default hard-coded passwords set by the vendor – passwords like “1234” and “admin”
    - Table activity: Cryptography
    - Table activity: Password strength
- Using very old versions of Windows that are susceptible to viruses from years ago. Hospitals have to use the older systems because some manufacturers will not allow their equipment to be modified with the newer versions, partially due to regulatory restrictions.
    - Table activity: Computer anatomy
- Embedded web servers and administrative interfaces that make devices obvious and vulnerable to a breach within the network
    - Wi-Fi network attacks

AGENDA

9:15 am	Presenters Arrival
9:30 am	Students Arrival Meet the Cyber Career Speakers
10:00-10:05 am	Welcome and Introductions Dr. Davina Pruitt-Mentle Jeffrey Wells
10:05 - 10:20 am	Setting the stage for scenario and activities/Video
10:20 - 10:40 am	Activity 1/ Rotation 1
10:43 - 11:03 am	Activity 2/ Rotation 2
11:05 - 11:25 am	Activity 3/ Rotation 3
11:27– 11:50 am	Activity 4/ Rotation 4
11:50 – 12:15 pm	Organize at Lunch Tables
12:15 – 12:35 pm	Activity 5 Lunch Keynote Speaker: Renee Forney
12:35-1:00 pm	Activity 6 Discussion of the CyberCrime, Thank You's and Evaluations

If you should find a lost student this will help you direct her.



Agenda with Notes

9:15 a.m.	Speakers arrive	We ask that speakers arrive on or before 9:15 a.m. You will check in at the registration desk and will be directed to your table. After reviewing the materials you should have time to grab some coffee and Danish that we will provide.
Arrival – 9:30 a.m.	Meet Cyber Career Speakers	Buses are scheduled to arrive between 9:30 and 9:45 a.m. It would be great if speakers could make themselves available to talk to students who arrive before 9:45. Quotes about why our speakers say their careers are cool will be shown throughout the room. Speakers can walk around the room or stay close to their assigned table. We will encourage students to take advantage of this time to introduce themselves to the speakers and ask a few questions. We will have coffee and refreshments for presenters in the AM The restrooms are indicated in the above map. Speakers can help usher students toward the appropriate tables. Students must be in their seats by 9:55 so that we can begin on time. Students are asked to stay at their assigned tables and rotate as a group as detailed in the schedule.
10:00 - 10:05 a.m.	Welcome and Introductions	Students will be welcomed and the organizations which have supported us with speakers will be introduced. Welcome and Introductions: Dr. Davina Pruitt-Mentle & Jeffrey Wells
10:05 - 10:20 a.m.	Setting the stage for scenario and activities/video	Logistics will be covered about how the day will proceed. An introductory video will be shown to set the stage for the cybercrime students will be asked to explore.

10:20 - 10:40.	Activity 1	Students will be pre-assigned starting tables and will rotate as a group as detailed in the schedule. We have allowed a few minutes between rotations; however, you are welcome to begin as soon as all ladies are seated and ready to begin. During the Activity 4 please thank students for being so polite and cooperative up to this point and remind them that there is still more to come.
10:43 - 11:03	Activity 2	
11:05 - 11:25	Activity 3	
11:27– 11:50	Activity 4	
11:50- 12:15	Organize at Lunch Tables	Groups will stay at the Activity 4 table for the luncheon speaker and lunch. Teachers and volunteers will be bringing the box lunches to the tables. Along with parents, chaperones and teachers, we ask speakers to remind students to "unwrap" their lunches as soon as possible so that noise is limited during the keynote speaker presentation. The lunchtime speaker is going to begin promptly at 12:15 so the students need to be in their seats, quiet and ready to pay attention. Setting the expectation after this last session will help us stay on schedule. No one is allowed to enter or leave the room during the keynote speaker session.
12:15- 12:35	Activity 5	Introduction + Lunch Keynote Speaker : Renee Foley
12:35- 1:00	Activity 6	Dr. Davina Pruitt-Mentle, Closure Solve the Cyber Crime, Q and A, Thank You's and Evaluations
1:00	Depart	Load Buses

This table lists the Table each presenter is assigned and the groups that each will interact with for each rotation.

Table	Presenter, Organization, Topic, Activity	START & Rotation 1	Rotation 2	Rotation 3	Rotation4
1	Lindsey Beaubien, NGC Computer Parts	Theodore G. Davis 1	Matthew Henson 2	Benjamin Stoddert 3	Theodore G. Davis 4
2	Harriette Julian, NGC Computer Parts	Theodore G. Davis 2	Matthew Henson 3	Benjamin Stoddert 4	Benjamin Stoddert 1
3	Emily Koo, MC Computer Parts	Theodore G. Davis 3	Matthew Henson 4	Matthew Henson 1	Benjamin Stoddert 2
4	Angela Corrieri, Startup Partners Cryptography	Theodore G. Davis 4	Theodore G. Davis 1	Matthew Henson 2	Benjamin Stoddert 3
5	Bianca McNair, NSA Cryptography	Benjamin Stoddert 1	Theodore G. Davis 2	Matthew Henson 3	Benjamin Stoddert 4
6	Rosalinda Musquiz, NSA Cryptography	Benjamin Stoddert 2	Theodore G. Davis 3	Matthew Henson 4	Matthew Henson 1
7	Sherri Ramsey, CyberPoint International USB Drives	Benjamin Stoddert 3	Theodore G. Davis 4	Theodore G. Davis 1	Matthew Henson 2
8	Monica Ellis-Gorham, MAXIMUS USB Drives	Benjamin Stoddert 4	Benjamin Stoddert 1	Theodore G. Davis 2	Matthew Henson 3
9	Rebekah Tervin, Smartronix USB Drives	Matthew Henson 1	Benjamin Stoddert 2	Theodore G. Davis 3	Matthew Henson 4
10	Cheryl Kinchen, IAI Lock Picking	Matthew Henson 2	Benjamin Stoddert 3	Theodore G. Davis 4	Theodore G. Davis 1
11	Mirka Vera, MC Lock Picking	Matthew Henson 3	Benjamin Stoddert 4	Benjamin Stoddert 1	Theodore G. Davis 2
12	Sarah Purdum, UMBC Lock Picking	Matthew Henson 4	Matthew Henson 1	Benjamin Stoddert 2	Theodore G. Davis 3

This table lists the starting position and rotations for each of the schools

WHO	Abbreviation/Group # Number of students/chaperones	START & Activity 1	Activity 2	Activity3	Activity 4 & Stay for lunch
		TABLE	TABLE	TABLE	TABLE
Theodore G. Davis 1	Theo Davis 1 9 students	1	4	7	10
Theodore G. Davis 2	Theo Davis 2 9 students	2	5	8	11
Theodore G. Davis 3	Theo Davis 3 9 students	3	6	9	12
Theodore G. Davis 4	Theo Davis 4 9 students	4	7	10	1
Benjamin Stoddert 1	Benjamin Stoddert 1 8 students	5	8	11	2
Benjamin Stoddert 2	Benjamin Stoddert 2 8 students	6	9	12	3
Benjamin Stoddert 3	Benjamin Stoddert 3 8 students	7	10	1	4
Benjamin Stoddert 4	Benjamin Stoddert 4 6 students	8	11	2	5
Matthew Henson 1	Matthew Henson 1 8 students	9	12	3	6
Matthew Henson 2	Matthew Henson 2 8 students	10	1	4	7
Matthew Henson 3	Matthew Henson 3 8 students	11	2	5	8
Matthew Henson 4	Matthew Henson 4 6 students	12	3	6	9

SCHOOL		School Teacher Lead
Theodore G. Davis		Tunisha Bowman
Benjamin Stoddert		Cynthia Panizzi
		Wanda Proctor
		Jonica Gaskill
Matthew Henson		Beth Levy
		Johnson
Central Office		Simone Young
Central Office		Diane O'Grady-Cunnif

Activities and Clues: Just in case you are curious about possible clues to the crime

Topic	Clue	Activity
Physical Security	Physical security is important! Being able to access a room makes it a lot easier to manipulate equipment, medical records, or other electronic devices. Even things locked with a padlock can be accessed. How easy is it to pick a lock or guess a combination? What recommendations does the team have for physical security access?	Lock Picking
Cryptography	Once the serial and model numbers of the pacemaker are known, someone could then reprogram the firmware of a transmitter, which would allow reprogramming of a pacemaker in a person's body. An encrypted message was sent with important information. Can you break the code? What recommendations does the team have for more secure codes?	Frequency Chart and Cipher
Steganography	Several pictures are presented. Which picture contains hidden information? How can you tell? Could you have detected the hidden message without the cryptographic instructions? How could you protect against this type of threat?	Which picture has the files?
Digital Forensics 1	What are potential ways for thieves to steal or copy important information? Today many companies do not allow electronic or storage devices to be taken into work. Several organizations/companies actually inspect coats, bags, and briefcases to make sure the policy is followed. Hidden USB drives can be planted in women's jewelry bag and/or brief cases. Can you find all the hidden storage devices? What recommendations would you suggest to protect against the threat of removable media such as thumb drives?	Find the USB drives
Computer Science 1	Evidence was found on the thief's work computers. The team will examine computers used by the medical staff to control the medical device. The team will want to make sure that the problem did not originate with the original instructions given to the medical device by the medical practitioner. Alternatively, they will want to examine if a malicious set of instructions were entered. However, they have been disassembled. Further investigation reveals parts are missing. What parts were missing? A key part of being a cyber investigator is not only seeing what is there, but also noticing what is missing.	Find the missing parts
Computer Science 2	Evidence was found on the suspect's home computer. However, the keyboard is missing. Is there another way to use the computer without a keyboard?	Makey Makey
Digital Forensics 2	Clues can be gathered by exploring the suspect's browser history and cookies. Although these can be deleted, luckily the cybercriminal was not that smart. See if you can find anything related to the crime in the history and cookies. Make sure to look at all browsers on the system. How could the thief have avoided leaving this information behind?	Browser History
Social Engineering	How did the thief get access to some of the files? In many cases, high tech gadgets and knowledge is not even needed. Tactics such as social engineering can be used to gather incredible amounts of information. Spoofing or disguising the caller's number and even their voice make these tactics even easier. Can you protect against the types of attacks we demonstrated?	Spoofing

Questions Students have asked about Cyber Security and Women STEM Professionals in the past

Students have asked these questions in the past. You may want to think about how you would answer these questions if asked.

Cybersecurity careers

- How is cybersecurity used in today's jobs? How does cybersecurity affect other jobs?
- What types of jobs are cybersecurity jobs?
- What are the job responsibilities in each of the cybersecurity fields?
- How many hours a day do cybersecurity employees work?
- How much do cybersecurity workers get paid?
- What kind of people do cybersecurity professionals work with?
- What courses should I take if I am interested in this field?

Connection of information assurance to other careers

- How does cybersecurity protect us?
- How will knowing about cybersecurity help me with my career?
- How can I become more familiar with how computers work?

Hackers

- How do you become a hacker? What do you need to know?
- What do hackers know? What do hackers do? What do hackers want from me?

Security of personal data and computers

- How are we protected on the internet?
- How do you keep information safe on the internet?
- How do the various computer programs work to protect my information?
- How do I protect my computer and information?
- How safe is my computer now?
- How do I get rid of viruses?

Women STEM Professionals

- What do you wear to work?
- Do you have a family? Is it hard to work and have a family?
- What benefits does your company offer?
- Do you travel?
- What hours do you work?
- How many women do you work with?

Directions

The Center for Business and Industry is on the College of Southern Maryland La Plata Campus
http://www.csmd.edu/About/campuses/laplata/building/BI.html

The campus address is 8730 Mitchell Road, P.O. Box 910, La Plata, MD 20646-0910
http://www.csmd.edu/about/campuses/laplata/directions.html

To La Plata Campus, from Baltimore and other locations north

- Take I-95 South towards Washington.
- Continue on I-95 SOUTH/I-495 Capital Beltway.
- From Route I-495 Capital Beltway exit at 7A. This is Route 5, heading south toward Waldorf and Leonardtown.
- Continue on Route 5 to where it meets Route 301.
- Drive south on Route 301 for approximately 12 miles to the traffic light at the intersection of Mitchell Road.
- Turn right on Mitchell Road proceeding approximately two miles, reaching the main entrance to the campus which is on the right. Approximately one-tenth of a mile from the main entrance is the second entrance.

To La Plata Campus, from Frederick, MD and other locations west

- Take I-270 S.
- I-270 S becomes Capital Beltway/I-495 E.
- From Route I-495 E Capital Beltway exit at 7A. This is Route 5, heading south toward Waldorf and Leonardtown.
- Continue on Route 5 to where it meets Route 301.
- Drive south on Route 301 for approximately 12 miles to the traffic light at the intersection of Mitchell Road.
- Turn right on Mitchell Road proceeding approximately two miles, reaching the main entrance to the campus which is on the right. Approximately one-tenth of a mile from the main entrance is the second entrance.

To La Plata Campus, from Richmond and other locations south

- From Route I-95 N, take exit number 104 toward US-301/Bowling Green/Fort A.P. Hill.
- Continue on US-301 N for approximately 47 miles.
- Turn left onto Mitchell Road proceeding approximately two miles, reaching the main entrance to the campus which is on the right. Approximately one-tenth of a mile from the main entrance is the second entrance.

Parking is available in Parking Lot 6 next to Business and Industry Building.