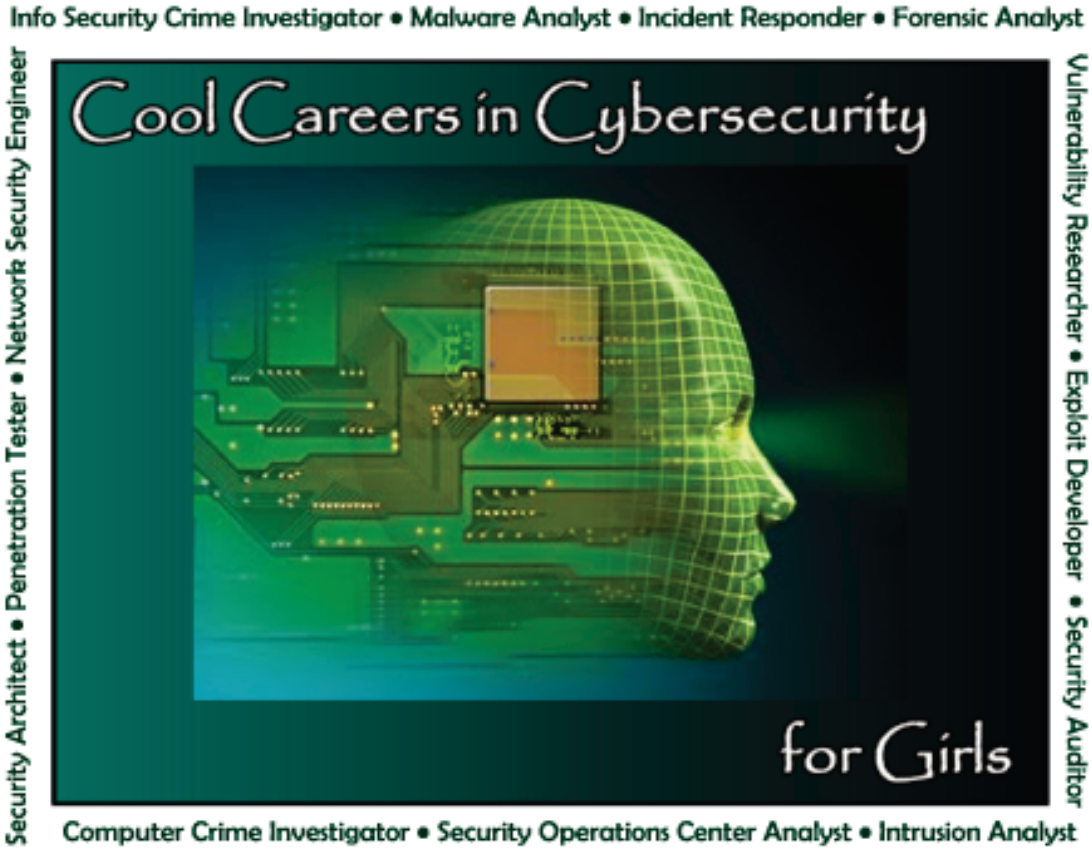


ETPRO

CyberWatch K12

www.edtechpolicy.org/cyberk12/

NSF

Cool Careers in Cybersecurity for Girls Workshop

November 14, 2012

10 a.m. to 1:30 p.m.

Riggs Alumni Center at the
University of Maryland - College Park, MD

MC2 Maryland Cybersecurity Center

The Cool Careers in CyberSecurity for Girls Workshop would not be possible without women professionals volunteering their time. Educational Technology Policy, Research and Outreach, the K12 lead of the National CyberWatch Center, in partnership with the University of Maryland, 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.

- Anne Arundel Community College
- Boeing
- Cisco
- DoD Cyber Crime Center (DC3)
- ISC2
- Lockheed Martin
- Lunarline
- Northrop Grumman
- NSA
- Radiant Blue Technologies
- SAIC
- Schnell-Tech Solutions
- Flexus: Women in Engineering Living and Learning Community -James Clark School of Engineering-UMCP
- University of Maryland University College (UMUC)
- Women's Society of Cyberjutsu

Please take the time to thank our wonderful professionals—please brief the girls to do the same.

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

Teacher Guide

Educational Technology Policy, Research and Outreach, the K12 lead of CyberWatch, in partnership with the University of Maryland, thanks you for your time and for bringing your students to the *Annual Cool Careers in Cybersecurity for Girls Workshop*. We know your time is valuable and there are many events for your students to attend. We appreciate your willingness to bring them to this event, and for all the time you put in to organizing on your end.

This teacher guide will help you prepare for the day. 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
- School Table start assignments
- Group table rotations

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 cybersecurity and STEM professionals and get clues to the crime.

The cybercrime scenario focuses on the growing problem of identity theft as experienced by a student, Anna Jimenez, and the difficulties it has caused for her and her family. The initial theft does not impact just Anna, but grows to include her siblings, and therefore affects the entire family.

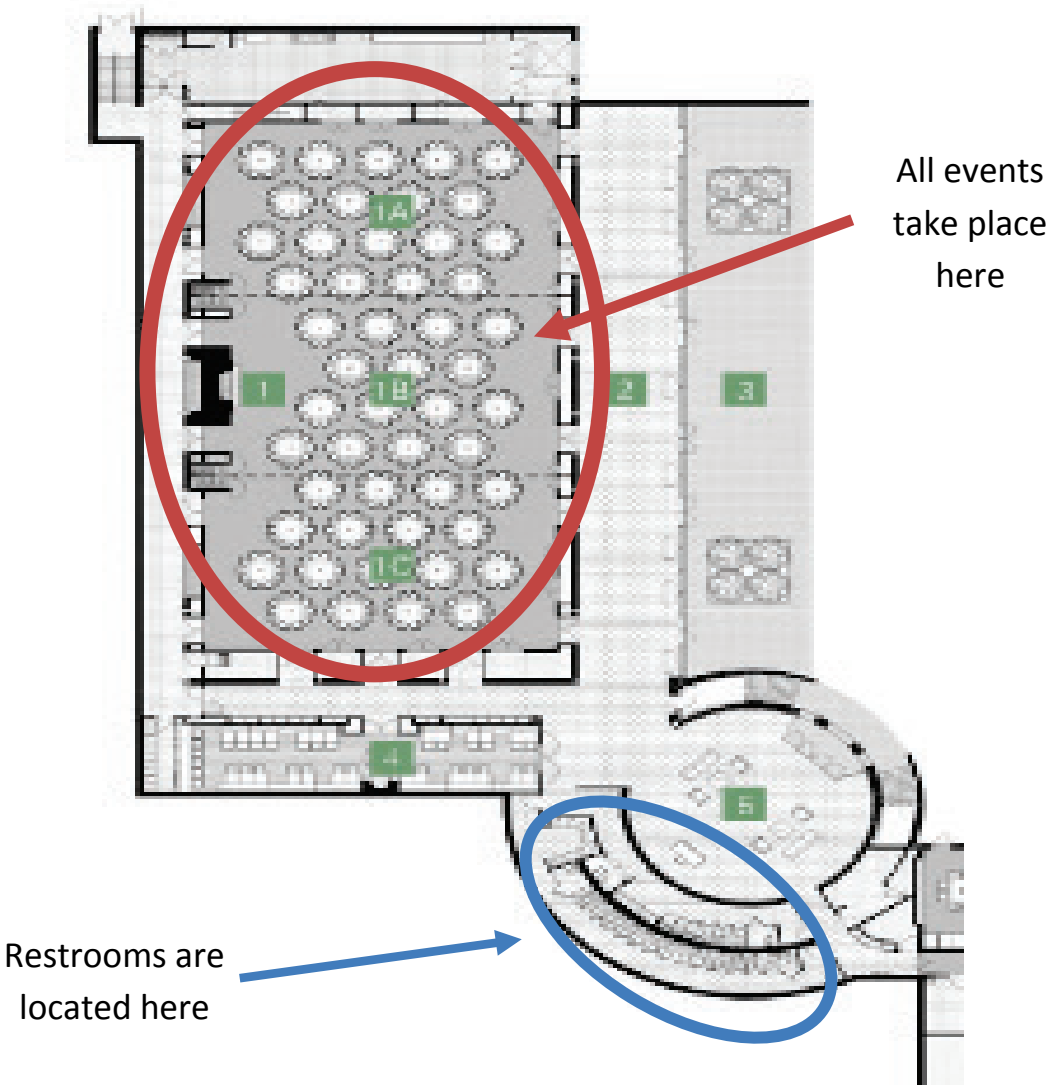
Anna's mom attempted to open a college fund savings account for Anna. She discovered that there was already an account with Anna's Social Security Number (SSN) and the account has a long and growing record of both cashing and writing bad checks. Later that week, Anna's brother Gabriel, who had just recently started college, received three different credit card statements and a telephone bill adding up to thousands of dollars –none of which were his.

The all girls' middle school Cyber Super-Investigators (CSI) will collect and explore a variety of cyber and physical evidence to learn more about how identity theft can occur. 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 solve the crime!

AGENDA

9:30 am	Arrival Meet the CyberCareer Speakers
10:00-10:15 am	Welcome and Introductions Dr. Davina Pruitt-Mentle Dr. Michel Cukier
10:15-10:25 am	Setting the stage for scenario and activities/Video
10:25 - 10:45 am	Activity 1
10:50 - 11:10 am	Activity 2
11:15 - 11:35 am	Activity 3
11:40 am - Noon	Activity 4
Noon - 12:20 pm	Organize at Lunch Tables
12:20-12:50 pm	Activity 5 Lunch Keynote Speaker: Dr. Jennifer Golbeck
12:50-1:15 pm	Activity 6 Solve the CyberCrime, Thank You's and Evaluations Board Buses

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



Agenda with Notes

Arrival – 9:30 a.m.	Meet CyberCareer Speakers	Buses are scheduled to arrive between 9:30 and 9:50 a.m. **Speakers will make themselves available to talk to students who arrive before 9:50.** Quotes about why our speakers say their careers are cool will be shown throughout the room. We will encourage students to take advantage of this time to introduce themselves to the speakers and ask a few questions. When arriving please take your groups directly to the pre-assigned tables (as indicated in this packet) The restrooms are indicated in the above map. 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 - 10:15 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 Dr. Michel Cukier
10:15 - 10:25 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 solve.

10:25 - 10:45.	Activity 1	Students will be pre-assigned starting tables and will rotate as a group as detailed in the schedule. **We have allowed 5 minutes between rotations; however, speakers are welcome to begin as soon as all ladies are seated and ready to begin.** **Students will stay at the last table (Activity 4) for lunch**
10:50 - 11:10	Activity 2	
11:15 - 11:35	Activity 3	
11:40– 12:00	Activity 4	
12:00- 12:20	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. We ask all parents, chaperones, teachers and speakers to remind students to "unwrap" their lunches as soon as possible so that noise is limited during the keynote speakers presentation. The lunchtime speaker is going to begin promptly at 12:20 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.
12:20- 12:50	Activity 5	Dr. Michel Cukier Introduction Lunch Keynote Speaker: Dr. Jennifer Golbeck
12:50- 1:15	Activity 6	Dr. Davina Pruitt-Mentle, Closure Solve the CyberCrime, Thank You and Evaluations
1:15	Depart	Load Buses

This table lists the starting position for each of the presenters

Table	Presenter, Organization, Topic, Activity	START & Activity 1	Activity 2	Activity3	Activity 4
1	Debra Curry & Melissa Thomas NSA Cryptography- Cipher	NO1 Group 1	NO2 Group 2	NO3 Group 3	NO4 Group 4
2	Dara Murray ISC2 & Kelly Rugel (UMD helper) Pen Testing/Malware - Computer parts	NO2 Group 2	NO3 Group 3	NO4 Group 4	NO1 Group 1
3	Colleen Calimer Boeing Sara McDermot (UMD helper) Systems Eng/Logic Model - OWN	NO3 Group 3	NO4 Group 4	NO1 Group 1	NO2 Group 2
4	Loyce Pailen UMUC Steganography Careers in cybersecurity/UMUC program OWN	NO4 Group 4	NO1 Group 1	NO2 Group 2	NO3 Group 3
5	Val Cash WSC & Kelly Chang NGC Cryptography Careers in cybersecurity, cipher	BL1 Group 5	BL2 Group 6	BL3 Group 7	BL4 Group 8
6	Lisa Foreman WSC Pen testing/Operations/Network Scanning OWN	BL2 Group 6	BL3 Group 7	BL4 Group 8	BL1 Group 5
7	Meghan Good SAIC Logic	BL3 Group 7	BL4 Group 8	BL1 Group 5	BL2 Group 6
8	Rosemary Shumba UMUC Steganography Careers in cybersecurity/UMUC program OWN	BL4 Group 8	BL1 Group 5	BL2 Group 6	BL3 Group 7
9	Megan Galvin LMC Cryptography - cipher	C1 Group 9	C2 Group 10	C3 Group 11	WW1 Group 12
10	Gail Schnell Schnell-Tech Solutions/WSC Pen testing/operations/network scanning computer parts	C2 Group 10	C3 Group 11	WW1 Group 12	C1 Group 9
11	Marlene Roush SAIC Logic	C3 Group 11	WW1 Group 12	C1 Group 9	C2 Group 10
12	Perri Nejib LMC OWN “In your Face” Book	WW1 Group 12	C1 Group 9	C2 Group 10	C3 Group 11

13	Dina Haines AACC Careers in cybersecurity/AACC program Recovering Files/Cryptography OWN	WW2 Group 13	WW3 Group 14	WW4 Group 15	WW5 Group 16
14	Andreae Pohlman WSC Pen testing/operations/network scanning Computer parts	WW3 Group 14	WW4 Group 15	WW5 Group 16	WW2 Group 13
15	Mary Phillips LMC & Jackie Weber (UMD helper) Logic OWN	WW4 Group 15	WW5 Group 16	WW2 Group 13	WW3 Group 14
16	Kelly Kline DC3 Steganography/Digital Forensics OWN	WW5 Group 16	WW2 Group 13	WW3 Group 14	WW4 Group 15
17	Simone Hunter & Mary Roy NSA Cryptography Cipher	FQ1 Group 17	FQ2 Group 18	SL1 Group 19	SL2 Group 20
18	Stacey Banks Oxford Federal/WSC Pen Testing/Malware Computer parts	FQ2 Group 18	SL1 Group 19	SL2 Group 20	FQ1 Group 17
19	Dawn Beyer LMC Logic	SL1 Group 19	SL2 Group 20	FQ1 Group 17	FQ2 Group 18
20	Sara Blount DC3 Steganography/Digital Forensics OWN	SL2 Group 20	FQ1 Group 17	FQ2 Group 18	SL1 Group 19
21	Sarah Zatko RadiantBlueTechnologies Cryptography - Cipher	Sligo1 Group 21	Sligo2 Group 22	Sligo3 Group 23	Sligo4 Group 24
22	Michelle Jackson WSC Pen Testing/Malware Computer parts	Sligo2 Group 22	Sligo3 Group 23	Sligo4 Group 24	Sligo1 Group 21
23	Dalila Wortman LMC Desira Stearns LMC Logic	Sligo3 Group 23	Sligo4 Group 24	Sligo1 Group 21	Sligo2 Group 22
24	Rose Kirby Lunarline Lock Picking	Sligo4 Group 24	Sligo1 Group 21	Sligo2 Group 22	Sligo3 Group 23

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	Activity 3	Activity 4
		TABLE	TABLE	TABLE	TABLE
Nicholas Orem 1	NO1 (1) 13 + 1	1	2	3	4
Nicholas Orem 2	NO2 (2) 13 + 1	2	3	4	1
Nicholas Orem 3	NO3 (3) 12 + 1	3	4	1	2
Nicholas Orem 4	NO4 (4) 12 + extra	4	1	2	3
Buck Lodge 1	BL1 (5) 13 + 1	5	6	7	8
Buck Lodge 2	BL2 (6) 13 + 1	6	7	8	5
Buck Lodge 3	BL3 (7) 12 + 1	7	8	5	6
Buck Lodge 4	BL4 (8) 12 + 1	8	5	6	7
Clarksville1	C1 (9) 13 + 1	9	10	11	12
Clarksville2	C2 (10) 13 + 1	10	11	12	9
Clarksville3	C3 (11) 14 + 1	11	12	9	10
William Wirt 1	WW1 (12) 15 + 1	12	9	10	11
William Wirt 2	WW2 (13) 15 + 1	13	14	15	16
William Wirt 3	WW3 (14) 14 + 1	14	15	16	13
William Wirt 4	WW4 (15) 14 + 1	15	16	13	14
William Wirt 5	WW5 (16) 14 + 1	16	13	14	15
Folly Quarter 1	FQ1 (17) 13 + 1	17	18	19	20
Folly Quarter 2	FQ2 (18) 13 + 2	18	19	20	17
St Louis 1	SL1 (19) 16 + 1	19	20	17	18
St Louis 2	SL2 (20) 16 + 1	20	17	18	19
Sligo 1	Sligo 1 (21) 13 + 2	21	22	23	24
Sligo 2	Sligo 2 (22) 13 + 1	22	23	24	21
Sligo 3	Sligo 3 (23) 13 + 1	23	24	21	22
Sligo 4	Sligo 4 (24) 14+ 2	24	21	22	23

SCHOOL	District	School Teacher Lead
Buck Lodge (BL)	PGCPS	Iris Schwarz
Clarksville	HCPS	Philip Herdman
Folly Quarter Middle School (FQMS)	HCPS	Heather Taylor
Nicholas Orem (NO)	PGCPS	Masaley Kargbo
St Louis Catholic School (SL)	Archdiocese of Baltimore	Zulma Whiteford
Sligo	Montgomery	Christina Campo-Abdoun
William Wirt (WW)	PGCPS	Stacey Montgomery

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

Topic	Clue	Activity
Systems Engineering/Logic	Observations indicate that there are numerous ways identity theft can occur, to include: dumpster diving, key loggers, shoulder surfing, weak passwords, and malware installed—through opening attachments or clicking on links. Students will review the list of evidence with a system's perspective to analyze what evidence is needed to identify the criminal. This connects with the analysis role of the systems engineer.	Logic models and flow charts
General	User name and password and other personal information was thrown away in a trash can. All examples but students will discover not related to the case	Dumpster diving
Law Enforcement/Digital Forensics	Anna's family recently got rid of an old computer but did not properly dispose of the hard drive. Anna's brother lost his cell phone and did not have it password protected. Proper procedures need to be carried out when handling evidence. Proper steps should be taken to protect personal information.	Computer parts Cell phones
Digital Forensics 1	Cell Phone with deleted files. Students will use a SIM card reader to retrieve deleted files from a cell phone. This can lead to a discussion about secure communications or the permanence of digital information. Example but students will discover not related to the case	Cell phone-SIM Card Reader
General	Physical security is just as important! Someone picked a lock and got into a school locker and stole a cell phone and other items. From this found facebook account that was already logged in and person posted mean comments pretending to be someone else Example but students will discover not related to the case	Lock Picking
Cryptography 1	Cracking weak passwords. Stolen cell phone and old computer includes a variety of information, notes etc. Students will decrypt a message using a frequency chart and cryptography wheel. Students will learn the importance of encryption in everyday life: UPC, credit card transactions, and texting. From this someone can find important bank and credit card information.	Frequency Chart and Cipher
Law Enforcement	A check looks like it has been changed. Example but students will discover not related to the case	Acetone check writing-ink
Penetration Testing	Clicking on images, unknown links or downloading files Learn about malware that can leave you vulnerable Investigate key logger file for evidence of a cybercriminal's identity.	Pen testing – operations - network scanning
Software Engineering	Someone has not installed/updated/turned on firewall—someone else has not updated OS or installed patches Example but students will discover not related to the case.	Malware
Forensics 2	Someone has posted a picture which looks like someone is breaking into a locker—the picture was actually false -pictures can be altered Example but students will discover not related to the case.	Use software to look for altered pictures
Networking	A packet sniffer was found on the computer connected to the router. Example but students will discover not related to the case	Networking exercise
Steganography	List of user names, passwords and other important information have been hidden within a picture file. Use software/ diagnostic tools to look for altered pictures. Inspect altered images for clues to the criminal's identity. Connections to digital forensic investigations will be explored. Example but students will discover not related to the case	Steganography files
Wireless	Students will access a wireless data stream and investigate the data. The vulnerability of wireless technologies will be connected to instruction on how to identify safe wireless hotspots. Example but students will discover not related to the case.	Wireless
Robotics	Students will program a "human robot" to retrieve a package. This activity links to a conversation about the many disciplines required for a successful robotics program including: electrical, and mechanical engineers and mathematicians and computer scientist. Example but students will discover not related to the case.	Programming
Malware	Students will perform diagnostics on a machine and find a key logger. Risky behaviors that put student data, information and identities in jeopardy will be explained.	Malware

Questions Students have asked about CyberSecurity 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 people create cybersecurity?
- How does cybersecurity protects 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? And what do they do? What do they 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 Samuel Riggs IV Alumni Center is on the University of Maryland College Park Campus http://www.riggs.umd.edu/

The Samuel Riggs IV Alumni Center does not have a physical address. If you would like directions to the facility from your starting address, please go to http://riggs.umd.edu/map.html

THE SAMUEL RIGGS IV ALUMNI CENTER is situated on the University of Maryland, College Park, campus—conveniently located off of I-495 and close to the College Park Metro Station. The center is at the hub of the university's northwest corner next to the Clarice Smith Performing Arts Center and Byrd Stadium. I would suggest (if coming off 95) exit onto Route 1 towards College Park. Exit onto Route 193. At the second traffic light, take a left onto Stadium Drive. Enter the round about—bear off first right (stadium Garage is on the left and so is the Riggs Alumni Center. If you get to a second round about—you've gone too far.

Parking is available in the Stadium Parking garage next to the Riggs Alumni Center. Cost is $3.00 /hr or $15.00 for the full day. You will park, remember you're parking # and pay at the parking booth. Please bring the receipt and turn it in to us with your full name, address and phone number printed on the back of receipt (or we will have forms to complete).