THE ELECTIONS GROUP

Accelerating Excellence

Cyber Navigator Resources Case Study

How the Virginia Department of Elections partners with local colleges and universities

VIRGINIA CYBER NAVIGATOR

Virginia's Cyber Navigator Internship Program

In 2016, malicious actors launched cyber attacks on voter registration databases within the United States. While there is no evidence that bad actors succeeded in infiltrating Virginia's voter registration system, attacks across the country alerted Virginia's election officials and lawmakers to the importance of cybersecurity in elections. In 2019, Virginia lawmakers mandated that local election offices meet minimum cybersecurity standards or risk losing access to the statewide voter registration database. The law aims to protect voter registration data by ensuring that only offices with adequate cybersecurity can access the state's voter registration database.

The Problem

Many local election officials do not have the staff, resources, or knowledge to secure their offices from cyber threats. Still, Virginia's local election officials could not risk losing access to the statewide voter registration database. Without access, local offices would not be able to perform many critical operations, including registering new voters and updating existing voter registration records. Virginia's local election officials needed a cost-effective way to meet statewide cybersecurity standards.

The Solution

The Virginia Department of Elections began searching for other state agencies that could help local election officials meet and exceed the state's cybersecurity standards. Fortunately, the University of Virginia (UVA) is nationally recognized for its excellence in cyber security. Leaders from the Vir-

ginia Department of Elections met with cybersecurity experts from the University of Virginia's School of Engineering and Applied Science to discuss how to improve election cybersecurity. This led to the creation of Virginia's Cyber Navigator Internship Program (CNIP) – a program that deploys interns with elections and cybersecurity training to help local election offices improve their cybersecurity.

Partnering with the Department of Elections, UVA was awarded a $3 million grant from the National Centers of Academic Excellence in Cybersecurity to develop CNIP, including building a cybersecurity course and internship. Now, many other Virginia colleges and universities are also part of CNIP. The program was developed with consideration of the Cybersecurity and Infrastructure Security Agency's (CISA's) "Election Infrastructure Security Funding Considerations." Like Illinois, Virginia followed CISA's guidance to ensure that the resulting cyber navigator program would make efficient use of resources.

Virginia deployed its first cohort of 32 CNIP interns in Summer 2022. Those interns served 17 Virginia localities during 10-week internships. As the University of Virginia's CNIP web page states, the program's aim is "assessing, improving, and maintaining the cybersecurity of local [voter] registrar's offices across the Commonwealth while simultaneously educating cybersecurity students."

Through the CNIP program, college and university students studying cybersecurity or related disciplines are trained to work in election offices. These students attend special training sessions to learn about election administration and cybersecurity, and a cybersecurity "boot camp" hosted by participating colleges and universities. Upon completing their training, those students become interns at local election offices throughout the Commonwealth of Virginia.

The program is mutually beneficial. During their 10-week internships, participating students gain valuable real work experience as cybersecurity practitioners in the context of election administration. They also receive a stipend as part of the program. Participating election offices receive 10 weeks of excellent work from skilled cybersecurity interns, who help local offices comply with cybersecurity requirements and focus on any other local cybersecurity priorities.

Localities are not required to participate in the CNIP, but participating localities have benefited from joining CNIP. For example, Henry County's IT director, Dr. Christian Youngblood, spoke with the Center for Tech and Civic Life about the advantages of working with CNIP interns, stating "[W]e worked on risk analysis, security policy, and contingency planning to ensure Henry County continues to provide a true democratic election."

Virginia's Approach

Establishing cybersecurity standards
Virginia's cybersecurity standards are developed and updated annually by the Voter Registration System Security Advisory Group. This group is legislatively mandated and consists of state elections staff, local information technology professionals and local election officials. The group sets cybersecurity standards that each local election office must meet annually to guarantee continued access to the statewide voter registration database. These standards are referred to as Local Election Security Standards (LESS), found on page twenty-six of this link.

Meeting those standards

The CNIP prepares students to assist their assigned jurisdictions with any cybersecurity priorities, including complying with the standards. Local jurisdictions that already comply fully with the standards can focus on maturing and improving their existing cybersystems.

Determining the program's scope

The standards cover a wide breadth of election security topics, including physical security. However, CNIP has a specific focus on improving local cybersecurity. CNIP is an ambitious program, and

compliance is not the only goal. The program aims to assess, improve and maintain the cybersecurity of any participating office across the Commonwealth, even if the office already meets or exceeds many cybersecurity requirements. Activities that interns might perform include:

- Risk assessments of information systems;
- Analysis of system and network documentation for accuracy;
- Guidance and assistance regarding software patches and system updates;
- Assistance configuring and deploying appropriate security software;
- Ensuring compliance with best practices in securing systems; and
- Helping to share relevant information with other local election officials.

Partnering with colleges and universities

CNIP is unique among cybernavigator programs for leveraging the knowledge and expertise of Virginia's colleges and universities and their students. Many of Virginia's public universities and colleges participate in the CNIP, including George Mason University, James Madison University,

Norfolk State University, Old Dominion University, Virginia Commonwealth University, and Virginia Tech. Participating colleges and universities host CNIP courses and provide interns for the program. The Department of Elections entered into a memorandum of understanding with these colleges and universities, knowing that the CNIP would mutually benefit university students and Virginia's local election offices.

Building a curriculum

The Virginia Department of Elections partnered with participating colleges and universities to develop a cybersecurity course called "Election Security." The course gives students lessons in both cybersecurity and election administration. Students enrolled in the course read and discuss foundational texts on both subjects. For example, the first cohort took instruction from the textbook Securing the Vote: Protecting American Democracy. They also read and analyzed other important documents, including Virginia's Election Laws, and election security materials from the federal Cybersecurity and Infrastructure Security Agency (CISA).

Students in the course receive instruction from professors and practitioners, including staff from the Virginia Department of Elections. The curriculum prepares those students to succeed while working in local election offices. For example, in 2022 the first lesson introduced students to elections in the United States, and subsequent lessons narrowed their focus to Virginia's elections. The course also refreshed students on cybersecurity principals like access control and intrusion detection.

Coursework also focuses on building practical skills. This includes instruction on security awareness and on performing risk assessments of local offices. As part of the course, students visit a local election office, where they learned more about the process of local election administration.

Preparing students to become interns

In addition to their coursework, prospective interns participate in a "boot camp" that provides final instruction before internships start. In 2022, the CNIP boot camp was a two-day program where future interns were housed in dormitories at the University of Virginia.

The 2022 boot camp brought together interns, professors, cybersecurity experts, and Department of Elections staff to meet in person. It was organized into panel sessions, including a presentation on safe and secure elections, team-building exercises, a refresher on the "Dos and Don'ts" of cybersecurity, a panel on professional behavior

and expectations, and more. A keynote speech was delivered by Kim Wyman, the Senior Election Security Advisor for CISA.

Creating a program that benefits localities and interns

Before starting their work, interns, their universities, and local election officials enter into Internship Agreements. Those agreements provide a record of the commitments that interns, universities, and local electoral boards have made pursuant to the CNIP. They include important details, like the internship start and end date. They also ensure that all parties understand the conditions necessary for a successful CNIP.

Promoting confidentiality and data privacy
Interns must sign confidentiality agreements before beginning their work at local election offices. Interns agree to protect important information and data stored in local election offices, as well as the information and data stored in Virginia's voter registration database. They agree to make all reasonable efforts to maintain the confidentiality of local security information. And they agree not to discuss meetings or work with persons who are not members of the CNIP. These promises protect confidential information, and they support a relationship of trust and confidence between interns and the local election officials who host them.

Identifying jurisdictions for CNIP participation

In 2022, Virginia's Department of Elections sent a communications advisory to all local offices explaining the CNIP and soliciting interest. The Department also encouraged certain localities to participate, including localities that needed assistance to comply with the Local Election Security Standards.

The Department of Elections considers many factors when choosing CNIP localities. The Department prioritizes local jurisdictions that have expressed interest in the program or whose election officials are excited to host interns. The Department also seeks to place interns in offices with experienced leadership. This ensures a good experience for interns and helps promote the CNIP to other local offices. Once offices have been chosen, CNIP matches interns with offices. Considerations for matching an intern to an office include the intern's proximity to the office, as well as whether the intern is a good skill match for that office's needs.

Risk assessment surveys help the Department of Elections identify local offices that are a good fit for CNIP. The Department issues annual risk assessment surveys to all local election officials to determine their current level of compliance with LESS. The survey asks localities which cybersecurity protections and tools they already have in place. For example, it asks each locality if they have an acceptable use policy, and how they provide security awareness and information security training. The results of this survey are used to identify localities that may need an intern's help to comply with LESS.

Doing the work

Once internships start, CNIP interns provide support to localities to achieve core compliance items and the locality's top cybersecurity priorities. Interns perform critical tasks like developing security plans, policies and procedures.

Interns serve for a 10-week period in the summer and work 30-hour weeks. The interns may work either remotely or on site, as needed. However, interns are required to travel to their local election office at least three times during the internship. This ensures that interns receive in-person experience at the local election office as part of the internship experience.

On August 22, 2022, the Center for Tech and Civic Life published a "spotlight" on Henry County and its participation in CNIP. On the first day of the internship program, the local office hosted a kick-off celebration for their interns, who were introduced to the office's equipment, technology, and laws and procedures. After that, interns primarily worked remotely and were able to provide high quality support to the local general registrar and her staff. During their

tenure, the Henry County interns worked with the general registrar's office on risk analysis, security policy, and contingency planning.

Henry County general registrar Dawn Stultz-Vaugn explained the importance of collaboration within the CNIP, stating "The elections department will likely have blind spots in their technology needs and the IT group will probably be unfamiliar with many of the Registrar's duties and responsibilities. Success will be greater if everyone works together."

Costs and Funding

The program is funded through a grant from the National Centers of Academic Excellence in Cybersecurity, which is managed by the National Cryptologic School at the National Security Agency. Each of the universities with a leading role in the CNIP coalition holds a current National Centers of Academic Excellence designation, which means those universities are meeting standards to produce the cybersecurity workforce needed by the nation.

Program costs include the staff time and resources to develop elements of the program, like the program curriculum. There is also a significant initial time investment required by leaders from both the state elections community and the public universities who will participate in the program. Other costs include the expenses associated with the bootcamp and the internship itself. In 2022, Virginia provided interns with a stipend, which made participating in the internship program competitive and desirable.

Impact

Jurisdictions achieve cybersecurity goals
The CNIP's first cohort of interns and local offices made major accomplishments. One locality made their first incident response plan and conducted an incident response tabletop exercise. Another office's intern helped prepare a networking diagram for the entire county, so that county officials can quickly identify connected systems and mitigate damage in the event of a cyberattack. Most participating local offices developed acceptable use policies. Some offices implemented their first multi-factor identification programs for systems access.

Karen Hoyt-Stewart, who serves as the Local Security Program Manager for the Virginia Department of Elections, observed that "the localities that participated in the program are now moving forward faster." These localities have made an extra commitment to mature their local office's cybersecurity.

Interns save local offices time and money

The CNIP provides excellent training to students before they become interns. By the time that interns are deployed to local election offices, they already have foundational knowledge and training in both cybersecurity and election administration. This alleviates the time and cost that local jurisdictions would invest in training a new employee or intern. It ensures that local election offices get the most out of the 10-week summer internship period.

Participants engage with their state and local communities

The CNIP leverages enthusiastic, bright students who are already part of Virginia's community through their colleges and universities. These students complete their internships with a better understanding of the hard work and dedication that election officials and information technology professionals put into each of Virginia's elections. Further, the CNIP connects some of the many parties working hard to ensure safe and secure elections in Virginia. CNIP brings together local and state election officials, university professors and students, and cybersecurity experts.

Startup Timeline

CNIP first launched during the 2021-2022 academic year, and interns were first deployed in the summer of 2022. Therefore, cybersecurity interns began their work about three years after Virginia's General Assembly passed the law requiring local election offices to meet certain cybersecurity requirements to maintain access to the statewide voter registration database.

Infrastructure Needs

Universities and/or colleges with cybersecurity experts

CNIP relies on professors from public colleges and universities to train its cybersecurity interns. These professors must equip each student-intern with the skills and knowledge to help local election officials improve their cybersecurity posture.

Virginia's Department of Elections formed partnerships with universities that had been nationally recognized for their cybersecurity programs, like the University of Virginia. The colleges and universities leading CNIP each hold at least one current National Centers of Academic Excellence (NCAE) designation in Cybersecurity. This means that the National Centers of Academic Excellence have found that each of these universities meets the standards to produce the cybersecurity workforce needed by the nation. Any state can view their own colleges or universities that have received an NCAE designation here.

Cybersecurity standards and a risk assessment tool

Virginia has developed its own security standards for local election officials through the Voter Registration System Security work group. The 2023 standards can be found starting on page twenty-six of the document linked here. These standards include an annual requirement to provide incident response training; annual risk self-assessments using a tool provided by the Department of Elections; password composition and password management standards; and data encryption requirements.

The above chart shows the Password Management requirements in Virginia's 2023 Locality Election Security Standards (LESS)

A key responsibility of CNIP interns is helping localities comply with the cybersecurity requirements in those standards. With this responsibility in mind, it is necessary for Virginia to maintain an assessment tool that can measure each local office's compliance with those standards.

For the 2022 cohort, Virginia used a commercially available cybersecurity assessment tool. Moving forward, Virginia plans to use a tool it developed that is tailored to the realities of a local election office. This tool will measure each locality's compliance with the baseline LESS standards developed by the VRSS work group, with the expectation that all localities will strive for 100% baseline compliance. The tool also offers more advanced assessments for localities that are at 100% baseline compliance but wish to further improve their cybersecurity.

Local election officials who want to participate and benefit from the program

The CNIP cohort served 17 of Virginia's 133 localities over the summer of 2022. These localities were chosen based on a number of factors, but one important factor was the locality's interest in the program. This is especially true at the program's start, when developing enthusiasm and community investment is crucial to the program's growth. In 2023, Virginia hopes to expand the program to 44 interns serving 22 local jurisdictions.

Advice for Success

A successful CNIP requires partnerships between election departments and colleges and universities. States can review the National Centers of Academic Excellence's list of cybersecurity designees. These colleges and universities would make excellent partners for an election cybersecurity program, and they may receive grant awards to serve the partnership.

A successful internship program needs enthusiastic participation from local election officials. To do this, election directors must communicate the value of these programs. For example, state directors starting a new program should give localities

TECH 8 Password Management		BASELINE	PREFERRED	PLATINUM
1	***Password Complexity***			
1.1	All system passwords to access elections workstations and systems are at least 14 characters in length.	•	•	•
1.2	Passwords must contain all of the following: upper case character, lower case character, number, and special character.	•	•	•
1.3	Passwords cannot contain whole or partial user names, user ids, or repeating strings (e.g. 12341234)	•	•	•
1.4	Prevent easily guessable passwords by comparing against a common password list before accepting the password.			•
2	***Password Management***			
2.1	Passwords are encrypted at AES 256 or higher when transmitted or stored.	•	•	•
2.2	Passwords are not shared.	•	•	•
2.3	Passwords are not displayed on screen on entry, are obscured while being entered, and cannot be unmasked.	•	•	•
2.4	Users authenticate with current password before changing to a new one. The previous 3 passwords may not be reused when resetting passwords.	•	•	•
2.5	Access to the password storage location is highly restricted.	•	•	•
2.6	All systems require passwords to be changed every 90 days.	•	•	•
2.7	All elections employees have and use a password manager approved and installed by authorized technology personnel.		•	•
2.8	Ensure that feedback for invalid credentials is vague and does not provide clues to why an authentication failed. If a user tries to log in unsuccessfully, they only receive a "Login Unsuccessful" message. Additionally, password composition is never displayed to an unauthorized user.			•

The above chart shows the Password Management requirements in Virginia's 2023 Locality Election Security Standards (LESS)

specific examples of work that interns can do, like performing risk assessments, developing acceptable use policies, and preparing incident response plans.

State officials must also emphasize the importance of confidentiality to interns, so that local election officials feel comfortable participating in the CNIP. Virginia requires all interns to sign a confidentiality agreement, which details the information that interns cannot share with anyone outside the program. Interns also receive confidentiality training at the CNIP boot camp.

Scalability

Virginia made all local jurisdictions aware of the CNIP and gave all local election officials an opportunity to show interest in the program. However, only 17 localities were chosen to receive the first cohort of CNIP interns. This allowed the Department of Elections to closely monitor the first cohort's experience and make any necessary changes to the program.

Moving forward, Virginia plans to expand the scope of the program as more students and local election officials become involved. CNIP has several partner colleges and universities.

A different state implementing a similar program could start by involving fewer universities, localities or interns, and then scale the program up as the community becomes aware of its value.

Media and Recognitions

Interns work on election cybersecurity; two from VCU are stationed in Henry County from the Martinsville Bulletin, published July 13, 2022.
Henry County, Virginia Participates in Cybersecurity Internship Program from the Center for Tech and Civic Life, published August 22, 2022.