Project Charter

Incorporating Cybersecurity into a Public Service Education

Last Modified
Wednesday, January 12th, 2022

Approved
Wednesday, January 12th, 2022
John Kingdon’s "policy window" recognizes a moment in time when a problem reaches maturity, there is a political will to address the problem, and feasible solutions to the problem are present.

Policy windows are not permanent—they may close if not acted upon. At this present moment, NICE, NASPAA, and its accredited programs can affect the future of cybersecurity through their own policy window.
Cybersecurity cannot be achieved by technologists and information security officers alone. This is as true at the organizational level as it is at the strategic level where partnerships between government, academia, and the private sector come together to address current and future cybersecurity challenges. The National Initiative for Cybersecurity Education (NICE) recognizes this throughout its guiding documents, statements, and values calling attention to the importance of innovation, collaboration, and a diversity of opinions.

NICE is led by the National Institute of Standards and Technology (NIST) in the U.S. Department of Commerce, and is a partnership between government, academia, and the private sector focused on cybersecurity education, training, and workforce development. In its recently published Implementation Plan, NICE recognized an objective to advocate for multidisciplinary approaches that integrate cybersecurity across varied curricula that support diverse learners from a variety of backgrounds and experiences (1).

The Network of Schools of Public Policy, Affairs, and Administration (NASPAA) is an international association of more than 300 institutional member schools that award degrees in Public Policy, Public Administration, or Public Affairs (2). Over half of NASPAA graduates go directly into public service (either government or the military) after graduation, with 36% of graduates going directly into state or local government (3). NASPAA’s accreditation process includes eligibility requirements, program self-evaluation, on-site visit, and review by the Commission on Peer Review and Accreditation (COPRA). NASPAA does not accredit undergraduate or doctoral programs.

This project team will advise and assist NASPAA accredited programs in the creation or improvement of cybersecurity curricula. This voluntary and collaborative project should be guided by stakeholders from NICE (leaders in cybersecurity from the government, academia, and private sector) and NASPAA (program faculty, leaders in the NASPAA organization, and affiliated professionals from the American Society for Public Administration). Through an iterative process, this team will organize information on the current state of cybersecurity curricula in NASPAA programs, identify the topics of greatest importance to students in NASPAA programs, and introduce (or improve) cybersecurity curricula for these students. Deliverables will be identified based on the needs of students and the capabilities of the programs themselves.

Project Team Description
Summary (the Elevator Pitch)

“One cannot educate every governor, senator, cabinet secretary, or public administrator on the ins and outs of cybersecurity—but one can take real steps to ensure that members of their staff have received a basic education in the topics most critical to their role.”

Statement of Purpose

The purpose of this project team is to advise and assist NASPAA accredited programs in the creation or improvement of cybersecurity curricula. This voluntary and collaborative project should be guided by stakeholders from NICE (leaders in cybersecurity from the government, academia, and private sector) and NASPAA (program faculty, leaders in the NASPAA organization, and affiliated professionals from the American Society for Public Administration).

This purpose aligns with NICE Strategic Plan’s Implementation Plan under the Transforming Learning to Build and Sustain a Diverse and Skilled Workforce Objective 2.2: “Advocate for multidisciplinary approaches that integrate cybersecurity across varied curricula that support diverse learners from a variety of backgrounds and experiences.”
**Projected Scope**

The scope of this collaboration should be limited to developing the cybersecurity knowledge and skills and competencies of students participating in a public service education, but it can also serve as a model for incorporating cybersecurity-related content into other disciplines.

NASPAA publishes an annual report which presents a snapshot of its students and graduates from the programs in the current accreditation cycle. Placement data provided by NASPAA shows that 54% of graduates go directly into public service (either government or the military), with 36% of graduates going directly into state or local government (3). Non-profit organizations are the second largest placement category for graduates at 20%. Non-profit organizations include specialized mission driven organizations benefitting the public good as well as authorities, districts, commissions, development corporations, and municipal departments that are essentially owned by the government but often operate with their own charters as independent agencies.

Topics including emergency management, data science, national security, and all-hazards planning may be referenced in this project but only to the extent that their inclusion does not take away from the objective of incorporating cybersecurity into the education of future public service leaders. It is out of scope for this project to include topics that are related to cybersecurity and are themselves their own fields of study.
The project should identify or develop the knowledge and skill statements and competencies which enable graduates to enter the public service workforce with a measurable understanding of cybersecurity topics. While these graduates may not have obtained an expert level of proficiency, they should understand cybersecurity topics and be able to communicate with executives as well as information security officers.

Additionally, the project should provide opportunities necessary for acquiring additional knowledge and skills and competencies that would make it possible for graduates to enter the cybersecurity field after graduation, including preparing students to acquire industry-recognized certifications. However, this project is not intended to draw prospective or current students away from a NASPAA academic degree or certificate program into a cybersecurity-related program.
The team’s final deliverables are dependent on the knowledge the team develops through its iterative process. The earliest deliverables will be a collection of resources that reveal students’ needs and the capabilities of NASPAA programs to help students learn cybersecurity knowledge and skills. These resources may be used to simplify future decision-making and could include a variety of different types of media or learning materials.

**Gather Data and Understand Needs**

The team will collect and organize data from NASPAA programs and professional development resources intended for entry-level public service professionals to determine the current state of cybersecurity curricula in NASPAA programs.

The team will collect and organize data from NASPAA programs to determine the potential opportunities and challenges that the programs may have in helping students learn cybersecurity topics.

The team will also collect and organize data from recent NASPAA graduates and senior leaders in the public service who are familiar with cybersecurity to determine the knowledge and skills or competencies that recent graduates should have for their own careers and the betterment of their organizations.

**Develop processes**

With an understanding of the curricula, the team will document and compare the topics covered by courses, modules, and syllabi and other teaching tools with the needs of employers.

The team will identify gaps between student needs (according to graduates and senior leaders) and the topics covered in the existing education resources.

**Proposed Solutions**

Preliminary discussions with NASPAA stakeholders yielded the following suggestions for project deliverables:

---

**Proposed Deliverables**
Discrete items or products

- Create a document that identifies the most relevant topics for NASPAA students (and why)
- Using the previous document, create a “Course Framework and Competencies” document
- Using the “Course Framework and Competencies” document, create a course with fully-realized learning objectives, course material, current events, and references
  - Develop a pre- and post-test for measuring learning
  - Courses may be intended for in-person, online, or hybrid learning
  - Hybrid or online options provide options for students at smaller programs or programs without a cybersecurity subject matter expert to use the forthcoming reciprocity agreement
  - Different courses for each NASPAA degree type may not be required
- Material for case competitions or simulation-based training

Strategic outcomes

- Create opportunities for students and graduates to highlight the impact of NICE Framework knowledge and skills and competences to employers as they begin internships and careers throughout government
- Create career pathways for academic programs to develop their own cybersecurity concentrations
- Provide students with foundational knowledge necessary to prepare for industry-recognized certifications
- Build on-ramps for graduates of NASPAA programs to enter the cybersecurity workforce after graduation

(Measurable) Educational outcomes

- Identify students’ who have been selected for relevant internships, research opportunities, or graduate positions that relate to cybersecurity and include them in a longitudinal survey for a few years following graduation to see how their careers have developed and how well their education prepared them for their profession
- Demystify the field and career of cybersecurity for NASPAA students
  - Pre- and post-test for students who enroll in a course created by through this collaboration
- Inform students and graduates of the role that leaders in public service at all levels of government have in achieving cybersecurity and cybersecurity’s impact on public service missions
Timeline for Project Development

November 5, 2021  
Submit draft charter to NICE and the leadership of the Transform Learning Working Group (WG)

Wednesday, December 8, 2021  
Charter is reviewed by WG with stakeholder support from NASPAA

Wednesday, January 12, 2022  
Charter is approved and project team launched

Monday, January 17, 2022  
Early recruitment for project members begins

-------------------------------------

Official announcements for the project

Wednesday, February 9, 2022  
Next Working Group Meeting

- Projects teams are entrepreneurial groups that tackle specific objectives or strategies in NICE’s Implementation Plan. This project addresses Objective 2.2: “Advocate for multidisciplinary approaches that integrate cybersecurity across varied curricula that support diverse learners from a variety of backgrounds and experiences.”

- Projects are intended as short sprints of approximately six months and are reauthorized as necessary. The first sprint will be a little longer than six months as the project is stood up, volunteers are recruited, and stakeholders are contacted.
[Project Name]
Meeting
[Date | Time]
[Meeting Access Information]

I. Roll Call
II. Review of Project Charter
III. Discussion: Actions Taken Since Last Meeting
IV. Discussion: New/Ongoing Action Items
V. Next Meeting Reminder
## References


All images sourced from the United States Architect of the Capital.
END OF CHARTER