National Initiative for Cybersecurity Education (NICE) Community Coordinating Council

Project Charter

Incorporating Cybersecurity into a Public Service Education

Last Modified

Wednesday, July 13th, 2022

—

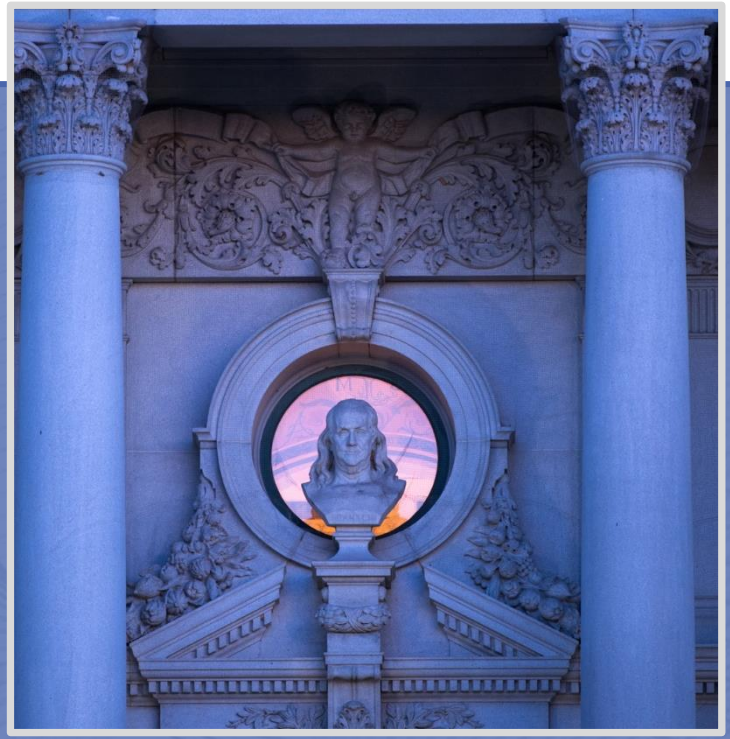
First Approved

Wednesday, January 12th, 2022

CALL TO ACTION

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, their partners can affect the future of cybersecurity through our own policy window.



Project Team Description

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 Purpose

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.

Project Team Objectives

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.

Previous Deliverables

January-June 2022

In its first six months the team organized members and processes, gathered information, and refined its goals and path forward. Major accomplishments in the first six months include:

1. Publishing and distributing a 6-page document intended to introduce the more than 300 NASPAA and more than 300 programs designated as National Centers of Academic Excellence in Cybersecurity (NCAE-C) so they may develop local partnerships.
2. Building a list of potential project partners and organizations that address similar issues around cybersecurity education and are also focused on NASPAA students and graduates, and public servants who did not graduate from a NASPAA program.
3. Submitting a presentation proposal which was accepted for the 2022 NASPAA conference to be held in Chicago this October.
4. Collecting and organizing resources on how to map syllabi to NCAE Knowledge Units and Knowledge Units to the NICE Framework.
5. Developing a "Rosetta Stone" document intended to be a translational reference for project members who come from a variety of backgrounds.
6. Developing and publishing a request for information (RFI) for NASPAA programs intended to collect information and resources that illustrate the current state of cybersecurity in NASPAA programs.
7. Presenting virtually to more than 40 attendees of NASPAA's comprehensive schools' program on the work of the project team, the use of the NICE framework, and an introduction to the NCAE Knowledge Units.
8. Presenting virtually to more than 60 attendees at NASPAA's career counselors conference on the NICE framework, the availability of cybersecurity certifications, and the skills presenters have found useful in data science and cybersecurity.
9. Proposing and launching an eight-week independent study program for four graduate students at Carnegie Mellon's Heinz College of Information Systems and Public Policy intended to tackle the following tasks:
    a. Enrich datasets and analyze the responses to the NASPAA RFI.
    b. Map syllabi to NCAE-C knowledge units, and knowledge units to NICE work roles.
    c. SWOT analysis to describe the challenges and opportunities facing NASPAA programs who wish to incorporate cybersecurity throughout their curricula.

Proposed Deliverables

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.

Publish a document answering the following critical questions

Based on expert insights, and the insights of and NASPAA graduates who now work in, or alongside the cybersecurity profession, what are the critical cybersecurity topics for NASPAA graduates, regardless of their career placement? This document must answer whether these topics currently taught in NASPAA programs. If yes, describe who, what, where, when, why, and how these topics are already taught in NASPAA programs.

For each instance of the team identifying potential project partners and organizations that address similar issues around cybersecurity education, the team should document the approach taken by other organizations. This document must describe their approach, any overlaps between other projects and this one, and how other projects developed their priorities or curriculum (where appropriate).

Report on "success stories" of NASPAA graduates who now work in, or alongside the cybersecurity profession

Are there examples of NASPAA graduates succeeding in cybersecurity work roles or careers adjacent to cybersecurity? If yes, these stories should be documented and shared with NASPAA programs. A standard suite of deliverable items should be developed that may include a head shot or professional photo, headline text, 2-3 pop out quotes, and 750-1,000 words describing graduates' stories and advice for NASPAA grads/programs.

Publish an organized list of statements and competencies focused on NASPAA students

These knowledge statements, skill statements, and competencies should enable NASPAA graduates to enter the public service workforce with a measurable understanding of cybersecurity knowledge, skills, and abilities most critical to their jobs. They must be based on data such as the insights gathered from experts and alumni.

Coordinate with subject matter experts to schedule a simulation-based cybersecurity training ahead of the 2023 NASPAA conference

Invite faculty, staff, or administrators supporting NASPAA programs to participate in or observe simulation style workshops based on real-world cyber events—like the workshops recently held at the American Society for Public Administration's 2022 conference.

Publish a document that provides programs with examples for incorporating cybersecurity throughout a public service education

The project team has previously described illustrations of what incorporating cybersecurity throughout a public service education may look like. This document must develop such illustrations into simple to understand and simple to implement approaches for faculty in NASPAA programs. These illustrations should be specific, measurable, achievable with the resources faculty are expected to already have, and relevant to the objectives of this project. This document must suggest a way for faculty to provide feedback to NASPAA and its partners.

Facilitate the publication of a cybersecurity related case study on publicases.org

The team will publish a case study or support another organization or individual in the development of a cybersecurity related case study.

References

1. **The National Initiative for Cybersecurity Education .** Implementation Plan. 2021.

2. **NASPAA.** About NASPAA. *NASPAA.* [Online] https://www.naspaa.org/about-naspaa.

3. **Maples, Kelli.** NASPAA Annual Data Report. 2021.

Library of Congress image credited to the United States Architect of the Capital

END OF CHARTER