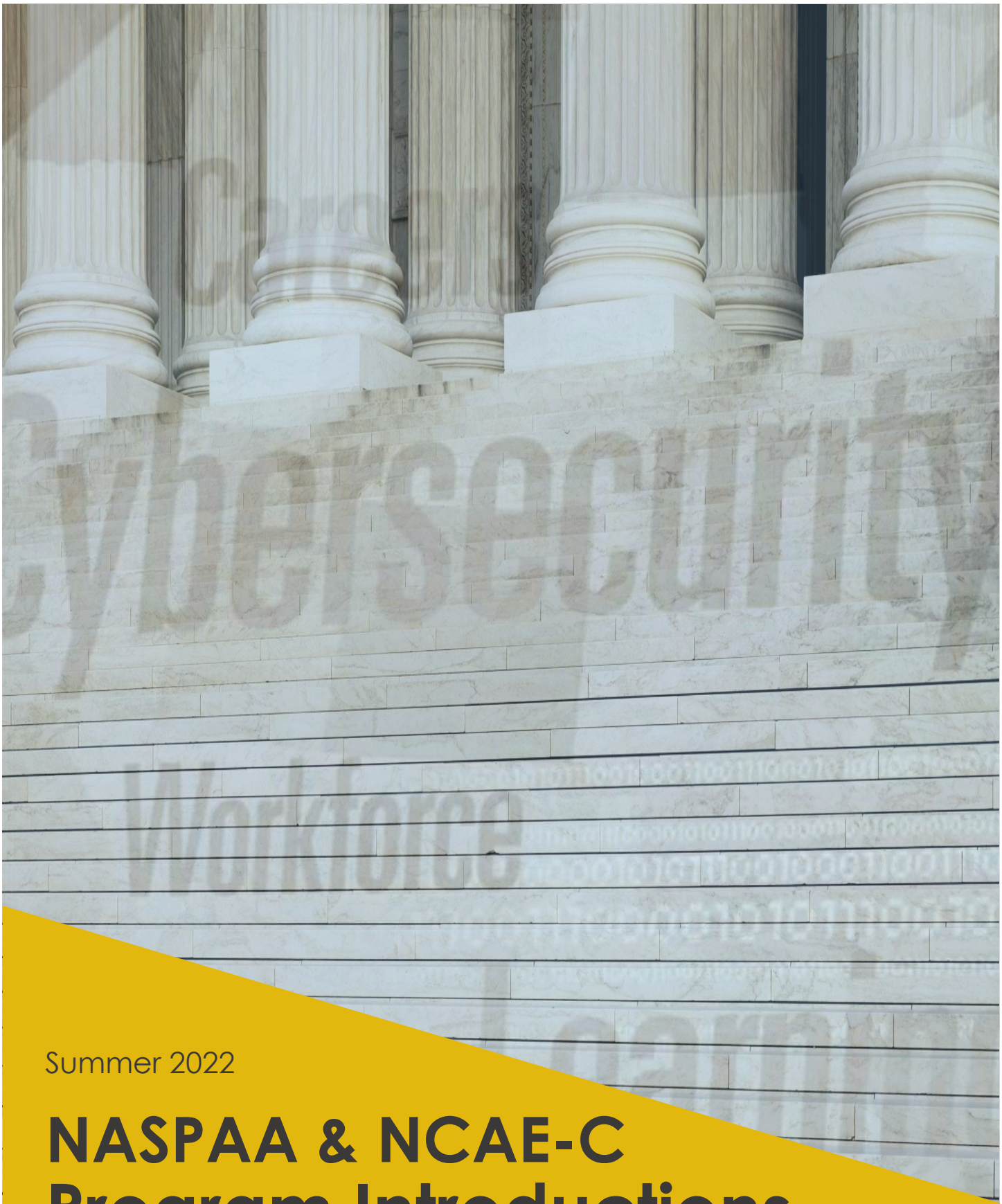

Summer 2022

NASPAA & NCAE-C Program Introductions

A publication by the NICE Community Coordinating Council's
Incorporating Cybersecurity into a Public Service Education Project Team

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 position."

Intent

This document is intended to be shared with the members of two organizations: the Network of Schools of Public Policy, Affairs, and Administration (NASPAA) and the National Centers of Academic Excellence in Cybersecurity (NCAE-C).

It is the hope of this project team that faculty, administrators, staff, and decision makers of all backgrounds—from both organizations—will become aware of the potential for partnership with programs on or near their campus and take this opportunity to introduce and open themselves up to local collaborations that provide tomorrow's leaders in government with the cybersecurity skills most critical to their position.

NASPAA is an international association of more than 300 institutional member schools that award degrees in Public Policy, Public Administration, or Public Affairs.

The **NCAE-C** program recognizes academic departments or research centers at more than 300 institutions in the United States, with designations in Cyber Defense (CAE-CD), Cyber Research (CAE-R), and Cyber Operations (CAE-CO).

There is no requirement or incentive for CAEs and NASPAA programs to make these introductions, or to develop local collaborations that better society or improve students' understanding of cybersecurity.

Programs which elect to connect and collaborate will be invited to share their stories and participate in future initiatives designed to recognize outstanding leadership and model multidisciplinary approaches that integrate cybersecurity across varied curricula to support diverse learners from a variety of backgrounds and experiences.

Background

This document is a deliverable of the "Incorporating Cybersecurity into a Public Service Education Project Team" on behalf of the National Initiative for Cybersecurity Education (NICE) Community Coordinating Council.

The NICE Community has been established to provide a mechanism in which public and private sector participants can develop concepts, design strategies, and pursue actions that advance cybersecurity education, training, and workforce development. The Community is comprised of four Community of Interest groups and three Working Groups (sponsoring five project teams) that meet independent of the NICE Community and report out at the NICE Community Meetings.

Projects teams are entrepreneurial groups, authorized in sprints of six months, that tackle specific objectives or strategies in NICE's Implementation Plan. This project team was launched by the Transform Learning Projects Working Group in January of 2022 to address Objective 2.2 of the NICE Implementation Plan: "Advocate for multidisciplinary approaches that integrate cybersecurity across varied curricula that support diverse learners from a variety of backgrounds and experiences."

As a fully volunteer project, with members spread across many industries and areas of practice, the team relies on members to self-select from the current taskings and coordinate their actions through the project co-chairs. Project members meet monthly to report updates, challenges, and new taskings.

Special thanks to the following members for their contributions to this document: Stacy Drudy, Director of Innovative Teaching and Learning, and Data Center Director at the Network of Schools of Public Policy, Affairs, and Administration; and Karen Leuschner, Program Manager, National Centers of the Academic Excellence in Cyber Defense. Design and layout of this document by Andrew Artz, Data Scientist at the National Institute of Standards and Technology.

The 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 NCAE-C, NASPAA, and its programs can affect the future of cybersecurity through their own policy window.

What does Incorporating Cybersecurity into a Public Service Education look like?

While cybersecurity in a NASPAA program may take the form of an elective course, the project team sees touch points to cybersecurity across all facets of a program. Consider the following illustrations:

"An instructor or TA in a course on government procurement, city management, or social services responds to an assignment or discussion post asking how Confidentiality, Integrity, and Availability factor into the students' proposals to purchase a new web service or provide open public data."

"Faculty, staff, or administrators supporting NASPAA programs are regularly invited 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"

"A career counselor knows there are more than 500,000 unfilled cybersecurity jobs. The counselor also knows where to find the resources that can help plan a workshop on cybersecurity and to find free or low cost training that students may complete and add to their resume."

"CAE and NASPAA programs collaborating to identify where aspects of foundational knowledge units are already being taught in NASPAA programs, or how current curricula maps to work roles in the NICE Framework."

If these ideas speak to you, and you would like to join the project or receive updates, please email:

NICEPublicServiceEducation+subscribe@list.nist.gov

Joining the Google Group will also provide access to project resources. The project team meets at 1:00PM (EST) Second Wednesday of every month.

Who are the National Centers for Academic Excellence in Cybersecurity?

The NCAE-C is managed by the Program Office at the National Security Agency. The NCAE-C aims to create and manage collaborative cybersecurity education programs with community colleges, colleges, and universities that:

- Integrates cybersecurity practice within the institution across academic disciplines,
- Values community outreach and leadership in professional development,
- Actively engages in solutions to challenges facing cybersecurity education,
- Establishes standards for cybersecurity curriculum and academic excellence,
- Includes competency development among students and faculty.

CAE are divided into regions, but a CAE based on one campus may serve a local network comprised of several institutions. Each institution may hold up to three designations but can validate additional programs that meet the same high standards required of CAE designated schools, thus producing a qualified workforce much needed by the nation. Beyond the classroom, CAEs offer faculty access to cybersecurity development training, and students the opportunity to apply for scholarships, access to career fairs, access to tech talk/forums on cybersecurity topics, and much more!

As part of their designation, CAE schools are also required to integrate Cybersecurity topics in additional disciplines within the school. So, what do the CAE designations mean?

Cyber Defense

The CAE-CD designation is awarded to regionally accredited academic institutions offering cybersecurity degrees and/or certificates at the associate, bachelor's, and graduate levels.

Cyber Research

Awarded to DoD schools, PhD producing military academies, or regionally accredited, degree granting four-year institutions rated by the Carnegie Foundation Basic Classification system as either a Doctoral Universities – Very high research activity, R2: Doctoral Universities – High research activity or D/PU: Doctoral/Professional Universities.

Cyber Operations

The CAE-CO program is a deeply technical, interdisciplinary, higher education program firmly grounded in the computer science, computer engineering, and/or electrical engineering disciplines, with extensive opportunities for hands-on applications via labs and exercises.

National Centers of Academic Excellence IN CYBERSECURITY

Attention NASPAA Programs!

Visit the following pages to learn more and locate a CAE near you

NCAE-C Website

NCAE-C Institution Map

Who is the Network of Schools of Public Policy, Affairs, and Administration?

NASPAA is an international association of schools that award Masters level degrees in Public Policy, Public Administration, Public Affairs, Non-Profits, and closely related fields of study. Over half of NASPAA graduates go directly into public service after graduation, with 36% of graduates going directly into state or local government (where cybersecurity skills are often critically behind the federal government).

NASPAA graduates are everywhere from state, local, tribal, and territorial governments to presidentially appointed and congressionally approved positions in CISA, DHS, and DOD. NASPAA representatives on the NICE project team recognize they cannot educate every governor, senator, cabinet secretary, or public administrator on the ins and outs of cybersecurity—but they can take real steps to ensure that members of their staff have received a basic education in the topics most critical to these roles.

In January, NASPAA partnered with NICE to begin to address the need to incorporate cybersecurity throughout a public service education. The objective of this project extends beyond the development of an elective course in cybersecurity, to thinking about where cybersecurity fits into existing courses, career counseling, academic research, and professional development.

NASPAA
The Global Standard in Public Service Education

NASPAA recently launched publicases.org, an online platform connecting students and faculty with case studies, data, and simulations. NASPAA is seeking to develop partnerships with schools in information technology, engineering, and computer science, and programs like the CAEs to make case studies and other engaged learning opportunities available to its students through Publicases.

The needs of the public sector are diverse, and so are the range of specialties covered by member schools. NASPAA accreditation is less prescriptive of curricula and more about ensuring public service professionals are receiving the highest quality of education, according to their program's mission statement; with a focus on the universal competencies' students should receive.

Accreditation includes eligibility requirements, program self-evaluation, on-site visits, and review by the Commission on Peer Review and Accreditation (COPRA). Because NASPAA accredits multiple degree titles, a university may have more than one accredited program—potentially in more than one school. NASPAA does not accredit undergraduate or doctoral programs, but these programs may be identified as NASPAA affiliates.

Attention CAEs!

Visit the following pages to learn more and locate the programs nearest to you

About NASPAA

NASPAA Roster of Accredited Programs

Innovative Teaching and Learning

What are the next steps?

Not every CAE or NASPAA program is alike… but those who wish to prepare the next generation of government leaders with the cybersecurity skills most critical to their position, who believe in multidisciplinary approaches to solving wicked problems, or who share in the vision that cybersecurity is not only the responsibility of technologists and information security officers, should seek out potential partners on or near their campus and take this opportunity to introduce themselves and explore local collaborations. The following ideas may help to break the ice or serve as a "jumping off point" for conversation.

Ideas for CAEs

Many NASPAA programs teach advanced methods courses and data analytics with Python or R. Consider inviting these students to workshops on Structured Analytic Techniques, or Open and All-Source Analysis.

Some NASPAA programs have specialties or concentrations in areas like Election Administration. Consider inviting these faculty to sit in on certain cybersecurity courses as a special guest or as guest lecturer.

An informal survey of NASPAA graduates found that those who took a cybersecurity course as an elective outside their school did not learn about FISMA, the role of OMB in cybersecurity, or how to respond if their organization was the victim of a ransomware attack. Consider collaborating with NASPAA programs and special interest student groups to design professional development and "train the trainer" workshops geared specifically for future policy analysts and public administrators.

Ideas for NASPAA programs

The objective of the NASPAA-NICE partnership is to extend cybersecurity education beyond the limits of elective courses. Consider inviting your career counselors, academic advisors, and student leaders to take part in introductions between the CAE and your program.

The needs and impacts of public servants extends beyond the topics typically published journals of policy analysis, management, and personnel administration. Consider whether research collaborations with CAEs may yield new insights or support the topics your faculty are already exploring.

Schools that house NASPAA programs often include additional programs in related fields, like All-Hazards Planning. These programs may have faculty with a wealth of experience around natural hazards but less experience around human based hazards like cyber-attacks—so consider inviting them to make introductions as well.