CAE in Cybersecurity Community Style Guide

Congratulations on receiving your designation from the National Centers of Academic Excellence in Cybersecurity (NCAE-C)! You are now part of an elite group, recognized for your superior standards and abilities to educate our future cyber workforce. Our national and economic security depends on expertise amongst the cyber workforce – not only at the National Security Agency (NSA), but also across our country, in all industries. Cybersecurity is a team sport; when one system is at risk, we are all at risk. NSA, along with its federal partners, highly values our well-educated cyber professionals.

The NSA, as an agent of the Department of Defense (DoD), the President of the United States, and ultimately the American people – has a duty to protect the information that lives on our National Security Systems, which handle the most sensitive data of the federal government and military.

As educators of the future cyber workforce, you are also at the forefront of keeping our nation safe. Our nation depends on your graduates, and you have proven yourselves worthy of that distinct role.

Now that you are a Center of Academic Excellence, designated by the NSA, you are part of the Centers of Academic Excellence in Cybersecurity Community (CAE-C Community). Within this community, you will have a place as a leader and collaborator, waving the flag for cybersecurity education.

NCAE-C designations began in 1999 with just a handful of institutions, and has grown to include hundreds of elite colleges and universities, as well as a number of federal and industry partners. Because of this growth, it is important the Community portrays itself accurately and consistently, so published communications must follow a community-wide standard. This Style Guide will help ensure consistency of language and visuals in official communications. In this guide, you will find guidance on logo usage and terminology to ensure uniform messaging for the NCAE-C program and the CAE-C Community. This will in turn support recruitment efforts and the relationship between academia, government, and industry.

Please use this as a reference tool to better understand the NCAE-C program and the CAE-C Community identity and how this identity should be maintained.

Please address any special design needs by contacting info@caecommunity.org.

Sincerely,

The National Centers of Academic Excellence in Cybersecurity and the CAE in Cybersecurity Community

National Centers of Academic Excellence in Cybersecurity

The National Centers of Academic Excellence in Cybersecurity (NCAE-C) program creates and manages a collaborative cybersecurity educational program with community colleges, colleges, and universities that:

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

Academic institutions may choose from three designations:

- ❖ **Cyber Defense (CAE-CD)** designation is awarded to regionally-accredited academic institutions offering cybersecurity degrees and/or certificates at the Associates, Bachelors, and graduate levels.
- ❖ **Cyber Research (CAE-R)** designation is 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 University – Highest Research Activity (R1), Doctoral University – Higher Research Activity (R2), or Doctoral University – Moderate Research Activity (R3).
- ❖ **Cyber Operations (CAE-CO)** designation 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.

The designation process is a combination of elements related to the institution, focused on outputs for determining academic achievement. This combination assures that the institution meets the desired characteristics of a CAE-C institution, and that the academic delivery to students is producing the qualified workforce needed by the nation.

Accepted Uses

The below uses for the name of the National Centers of Academic Excellence in Cybersecurity program should be used only in reference to the overarching program and the Program Management Office. Otherwise, reference the CAE-C Community. A good way to know whether to use 'NCAE-C' or 'CAE-C' is to determine if the name could be replaced with 'the program.' If it can, use NCAE-C, and if it cannot, use CAE-C. **NCAE-C refers only to the overall program and its administrative office, and not to any designation, institution, or publications in the broader Community.**

National Centers of Academic Excellence in Cybersecurity

This is the most formal name for the program. It is important to highlight that the program is national, therefore, use the formal name in publications, press inquiries, or for formal occasions. It is also customary to use this full name for the first text reference in any formal communications materials. The formal name clearly identifies the program and establishes a reference point for the less formal names to follow. Typically, this name is onl1 y used once as the full formal reference.

NCAE-C

This is an informal name for the program. This should never be used as the first text reference, but is acceptable for any subsequent references. This name is typically used to generally talk about the program.

NCAE

This is the most informal name for the program. This should never be used as the first text reference, but is acceptable for any subsequent references.

Program Management Office, PMO

This is used colloquially in reference to the administrative arm of the NCAE-C program at NSA, and is an informal name for the program. This should never be used as a substitute for the above accepted naming uses for the NCAE-C program in published materials.

Centers of Academic Excellence in Cybersecurity Community

The Centers of Academic Excellence in Cybersecurity (CAE-C) Community is the organized group of community colleges, colleges, and universities that hold a designation from the National Centers of Academic Excellence in Cybersecurity (NCAE-C) program. The mission of the CAE-C Community is to provide institutions designated by the NCAE-C with resources to aid in individual success through workshop facilitation, marketing efforts, and communication tools. The CAE-C Community actively engages with government representatives to provide educational workshops, opportunities for funding, conferences, and working groups. The Community also partners with industry to ensure that students entering the next generation cyber workforce have the necessary knowledge, skills, and abilities for a successful career in cyber.

Accepted Uses

The below uses for the name of the Centers of Academic Excellence in Cybersecurity Community should be used in reference to the CAE-C Community. A good way to know whether to use 'NCAE-C' or 'CAE-C' is to determine if the name could be replaced with 'the program.' If it can, use NCAE-C, and if it cannot, use CAE-C. NCAE-C refers only to the program office, and not to any designation, institution, or publication in the broader Community.

Centers of Academic Excellence in Cybersecurity Community

This is the most formal name for our community. It is important to highlight our role as Centers of Academic Excellence. Therefore, use our formal name in publications, press inquiries, or for formal occasions. It is also customary to use this name for the first text reference in any formal written correspondence. Our formal name clearly identifies who we are as a community and establishes a reference point for the less formal names to follow. Typically, this name is only used once as the full formal reference.

CAE in Cybersecurity Community

This is the acceptable, alternate formal name for the community. It is acceptable as a first text reference as well as any subsequent references. It is best to use this name when speaking with individuals that are familiar with the Centers of Academic Excellence Program.

CAE-C Community

This is an informal name for the community. This should never be used as the first text reference, but is acceptable for any subsequent references. This name is typically used to generally talk about the Community amongst the Community.

CAE

This is the most informal name for the community. This should never be used as the first text reference, but is acceptable for any subsequent references. This name is not only associated with our community, but other Center of Academic Excellence programs as well, therefore, this name should never be used as a first text reference and should always follow the formal naming conventions.

The Community

This is an informal name for the community. This should never be used as the first text reference, but is acceptable for any subsequent references. This name is not only associated with our community, therefore, this name should never be used as a first text reference and should only follow the formal naming conventions.

Preferred Terminology & Usage

Accreditation

When a cybersecurity program applies and meets the CAE-C requirements, it is NOT accredited, but designated. Accreditation is a review of the quality of a higher education institutions and programs, ensuring they meet minimum quality standards. Accreditation reviews in the U.S. are carried out by independent entities, not the government.

CAE Candidates Program National Center

Acts as the entry point for all colleges and universities that plan to apply for either academic validation or designation. It provides mentoring, resources, advice, and other support to colleges and universities that want to earn a designation, or to have their academic program validated as a first step in the process. Whatcom Community College is the lead institution.

CAE Competition Program

An initiative that aims to increase student and faculty engagement with cybersecurity competitions through an intuitive sequence of tools, tutorials, and activities that simplify and focus preparation activities within student clubs. The lead institutions are Mohawk Valley Community College and University of South Florida-Cyber Florida.

CAE Cybersecurity Workforce Development Program

An initiative through which certificate-based workforce development programs will be developed. This initiative involves pilot programs from the University of Louisville, Purdue University Northwest, and the University of West Florida, along with a number of coalition partners.

CAE in Cyber Defense, CAE-CD

The designation a school has for its Cyber Defense program. The designation should be referenced in one of these two ways. It was previously called a designation in "cyber defense education," but the term "education" was removed to be consistent with the CAE-CO designation.

CAE in Cyber Operations, CAE-CO

The designation a school has for its Cyber Operations program. The designation should be referenced in one of these two ways.

CAE in Cyber Research, CAE-R

The designation a school has for its Cyber Research program. The designation should be referenced in one of these two ways.

CAE in Cybersecurity Community National Center (CNC)

Offers three primary functions to the all CAE institutions: 1) provide technical and logistical support for CAE events, activities, and curriculum; 2) provide a portal for CAE Community resources, geographic regions, and the nation as a whole; 3) engage and facilitate strategic initiatives for the nation in the areas of research, student and faculty development, diversity, and other workforce development activities. Administered through California State University, San Bernardino (CSUSB).

CAE Initiatives

Efforts aimed to advance the functioning of the CAE-C Community and to organize and consolidate efforts to improve cybersecurity educational opportunities across the country.

CAE Peer Review National Center

Works with NCAE-C to train reviewers and execute peer reviews of applications for academic endorsement and/or designation. The lead institution is Northern Virginia Community College.

CAE Regional Hubs (CRH)

CAE-C Community institutions that serve as a central point for their respective geographical areas amongst other CAE schools. CRHs serve to coordinate and expand cybersecurity workforce initiatives throughout the country. There are five CRHs: 1) Northwest Regional Hub – a consortium of Capitol Technology University, Mohawk

Valley Community College, and Towson University; 2) Southeast Regional Hub – a consortium of the University of West Florida, University of South Florida-Cyber Florida, and Forsyth Technical Community College; 3) Midwest Regional Hub – Moraine Valley Community College; 4) Northwest Regional Hub – University of Colorado, Colorado Springs; and 5) Southwest Regional Hub – San Antonio College.

Community of Practice, CoP

The CAE-C Communities of Practice are groupings of designated institutions by designation type. Each CoP is led by an institution or pairs of institutions selected competitively bi-annually. The CoP provides recommendations to the CAE-C Program Office as to strategic planning and programs to facilitate continuous improvement of the program and the participating institutions.

Competency

The ability to perform a task in the context of a work role, as defined by the NICE Framework. These work roles use Blooms Taxonomy for the writing of tasks, knowledge, and skill statements.

Consolidated CAE-C Professional Development Resources

An initiative that will work to provide students with insight into careers in cybersecurity, professional behavior and ethics, and other soft skills in demand in the workplace.

Curriculum

Courses or a set of courses offered by an educational institution. In the context of the NCAE-C program, "curriculum" includes all course materials included in a program of study, such as texts, labs, exercises, or other educational activities.

Cybersecurity

Should always be written as one word. Colloquially, the term "cyber" is also acceptable. The Department of Defense uses "cyber" interchangeably with "cybersecurity," however, cyber encompasses more operational and security functions than just cybersecurity.

Cybersecurity Education Diversity Initiative, CEDI

An initiative aimed to increase the availability of cyber education programs at minority serving institutions (MSI). It involves developing credit transfer agreements between institutions with cyber degree programs and MSIs and sharing existing courses with MSIs who wish to offer them. The initiative also aims to create methods by which instructors at MSIs may participate in development opportunities, or instructors from existing programs can serve as guest lecturers at MSIs. The lead institution is Fordham University, who is working with several coalition partners.

Cybersecurity Faculty Development Program

An initiative aimed to coordinate a unified program to: 1) expand the knowledge and teaching qualifications of existing faculty; 2) recruit and provide pedagogical preparation for professors of practice; 3) recruit graduate students, particularly PhD candidates to teach cybersecurity; and 4) recruit transitioning military and civil service personnel from government to cybersecurity work roles.

Designation vs. Validation

When an institution wishes to become a CAE, the process begins with getting the program of study validated, with the submission of items, such as the curriculum, faculty profiles and qualifications, and the maturity of the program. Once the program of study has been validated, the institution may pursue a designation from the NCAE. A validation does not denote a designation.

Evidencing Competency Oversight Program

An initiative involving three efforts: 1) regional cybersecurity exercises; 2) a security situation center for evidencing competency; and 3) an evidencing competency working group. The lead institution is Norwich University.

Framework

Often used to refer to a set of guidelines (in lieu of “standards”) for preparation of curriculum, labs, or other educational materials or program elements. A framework used in the context of CAE-C is established using collaboration among the designated institutions in coordination with the CAE-C program office and federal partners, and finally adopted by CAE-C program office policy. See also “NICE Framework.”

Knowledge Units, KUs

A coherent defined block of knowledge related to cybersecurity, used to describe academic requirements for designation and are used to frame the description of a program of study. Matching an institution’s program of study academic outcomes to the collective outcomes of a set of KUs results in validation of NCAE-C academic requirements as the first of two steps to designation in cyber defense, cyber operations, or cyber research.

NCAE-Designated vs. CAE-Designated

While these terms are often interchangeable (and either is acceptable), they have slightly different connotations. If you are speaking about your school's designation as a way of showing that your school has a CAE-CD, CAE-R, or CAE-CO designation, use CAE-designated. If you want to show that the NCAE-C program has designated your school as part of the national program, use NCAE-designated.

NICE Framework

National Institute of Standards and Technology (NIST) Special Publication 800-181 revision 1, the Workforce Framework for Cybersecurity (NICE Framework), provides a set of building blocks for describing the tasks, knowledge, and skills that are needed to perform cybersecurity work performed by individuals and teams. Often referred to as "the Framework," the NICE Framework is used in the context of the NCAE-C program to map programs of study to competency objectives for students pursuing cybersecurity careers.

Partners (Federal)

NSA's National Cryptologic School (NCS) manages the NCAE-C program, but the program has two federal partners that make it possible: the Cybersecurity and Infrastructure Security Agency (CISA), which is part of the Department of Homeland Security (DHS), and the Federal Bureau of Investigation (FBI). NCAE-C also closely collaborates with other federal agencies: the National Initiative for Cybersecurity Education (NICE), a Department of Commerce organization, and the National Science Foundation (NSF).

Regions Investing in the Next Generation (RING), CAE K-12 Pipeline Program

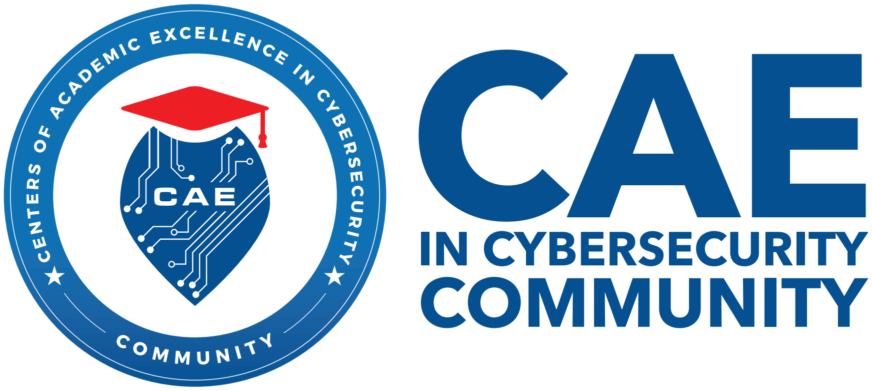
An initiative aimed to establish a CAE K-12 pipeline that will provide an online cybersecurity fundamentals course, which will target rural, under-resourced school systems, homeschool students, and schools without an established cybersecurity program. The lead institutions are the University of Alabama in Huntsville and Moraine Valley Community College, along with a number of coalition partners.

Senior Military College Cyber Institutes

An initiative aimed at create a deliberate pathway, enabling talent development in cyber and cyber-related competencies at senior military colleges (SMC) to meet Department of Defense (DoD) workforce needs for the near term and future emerging cyber challenges. This will be done by: 1) creating cyber institutes within senior military colleges; 2) expanding and sustaining cyber experiential programs; 3) recruiting, training, and deploying RC SMC deputy directors; 4) Extending persistent cyber training environment to SMCs; and 5) Building governance and assessment framework/processes. The lead institution is Norwich University.

Logos

The CAE-C and NCAE-C logos are a graphic representation of our community which distinguish us from other centers of excellence programs. They are designed to highlight our identity as cybersecurity educators and professionals, as well as our commitment to produce qualified cybersecurity professionals that will protect and defend the nation's infrastructure. Our logos also highlight our role within the industry of cybersecurity by distinguishing us from other CAE programs.



There are several main elements to the Centers of Academic Excellence in Cybersecurity Community visual identity:

- The design of the icon
- The design of the nameplate
- The full logo (icon and nameplate)
- The lettering style (or font)
- The correct colors
- The correct size, proportion and spacing
- The correct background

No logos other than the official Centers of Academic Excellence in Cybersecurity Community logo and those logos recognized as officially approved logos are authorized for use on any letterhead, business cards, publications, websites, or other applications representing the community or a unit of the community. A wide variety of accepted uses of the logo have been accommodated, allowing flexibility in how we present our visual identity. However, all uses of the logo must follow the guidelines set forth in this manual, and if altered such uses must be approved by the community's Program Manager (info@caecommunity.org) or the NCAE office (CAEPMO@nsa.gov).

Usage Rules

- Do not change the color of the logo (accepted: full color, black and white (CAE only), white);
- Do not lighten or darken the logo;
- Do not alter the text, color, or design of the logo;
- Do not use the logo in outline form;
- Do not add an outline to the logo;
- Do not distort, skew, morph or italicize the logo;
- Do not alter the proportions or spatial relationships of the logo or its elements;
- Do not add dark, harsh shadows as they may change the logo design;
- Do not use dimensional effects (i.e. three-dimensional or digital embossing effects);
- You can use the icon as a stand-alone image (icon only) where appropriate;
- Do not make a pattern or decorative device out of the logo or its parts;
- Do not use any part of the logo or its styling as the basis for another design;
- Ensure there is enough contrast between the logo and its background to be legible;
- Avoid busy, complex backgrounds that interfere with legibility;
- Do not use a logo unless it is in perfect condition (no blurriness, missing parts, etc);
- Also, please note, within the icon, the shield is on a white surface. The center of the logo is NOT transparent. Do not alter color.

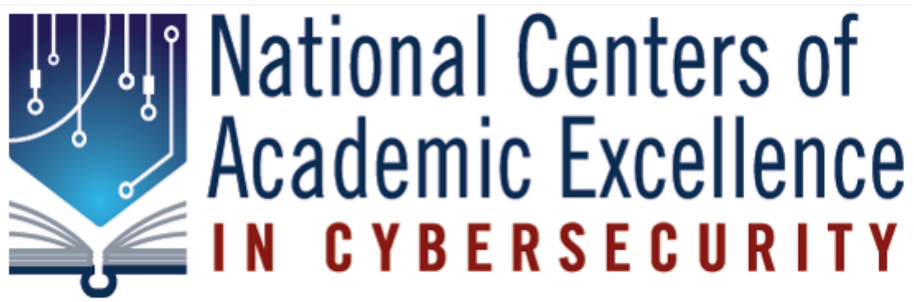
If you need any assistance or clarification of the guidelines, please contact the CAE in Cybersecurity Community Program Manager (info@caecommunity.org or 909-537-7535) or the NCAE office (CAEPMO@nsa.gov or 410-854-6206).

Please refer to the sample logos on the following pages for proper usage.

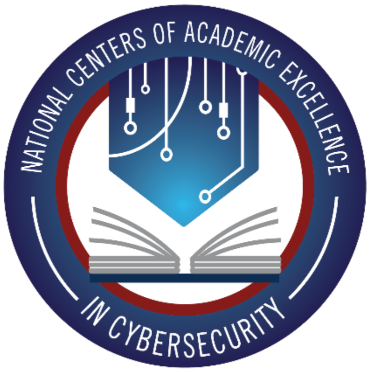
The NCAE in Cybersecurity Seal/Logo

The NCAE in Cybersecurity seal and logo are the graphical representation of our program and distinguishes us from other centers of excellence programs. It is designed to highlight our identity within cybersecurity education. The logo is comprised of two main parts, a stylized book and a shield. The book, which represents knowledge and education, opens up its pages to reveal a shield covered in cyber nodes. Cyber nodes are connection points in networks which this logo uses to represent cybersecurity. Together the book and shield create the NCAE-C banner logomark. The seal/logo should appear only on print/web/marketing materials that are directly produced by or connected to the PMO, and not on general Community materials.

Please follow all guidelines listed above for both logos. If you need any assistance or clarification of the guidelines, please contact the NCAE Program Office (CAEPMO@nsa.gov).



Logo



Seal

Font

The fonts used for the National Centers of Academic Excellence in Cybersecurity logo are Trade Gothic LT Std, Condensed No. 18 and. The text size will depend upon the size of your logo.

Blue Rim with White Lettering
R0 | G40 | B86
C100 | M84 | Y36 | K38
Hex #002856

Red Inner Rim
R135 | G29 | B25
C28 | M98 | Y100 | K34
Hex #871D19

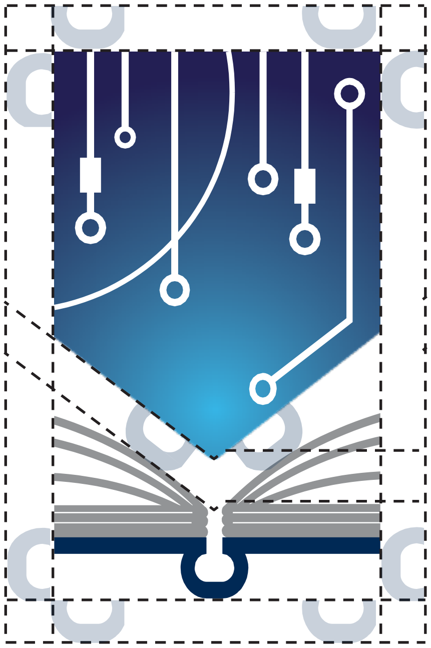
Order of Precedence

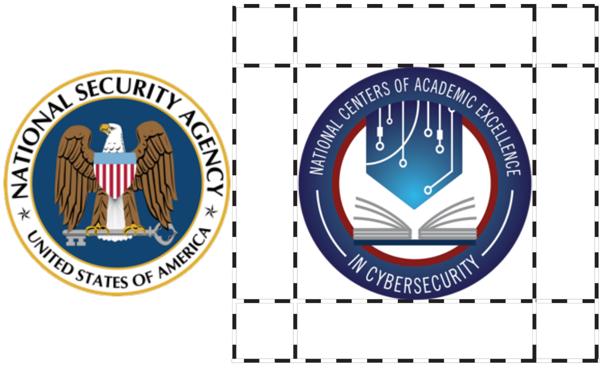
When pairing the NCAE-C Seal with the NSA seal, the NSA seal will always be displayed in front of the NCAE-C seal. Any NCAE-C affiliated logos (Community, Mentoring, etc.) should follow the NCAE-C Program logo/seal.

Note: If you currently hold a designation granted by the National Centers of Academic Excellence in Cybersecurity from the National Security Agency (NSA), you are permitted to use the NSA seal on relevant materials, such as your cybersecurity program's web site.

When spacing the NCAE-C logo with other artifacts, there must be a buffer zone of at least one 'book spine.'

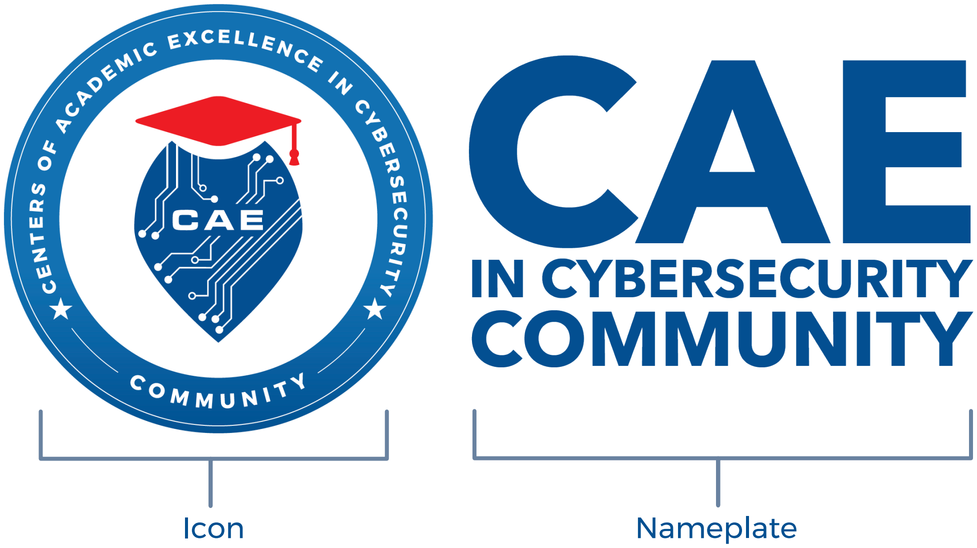
When spacing the NCAE-C seal, the buffer zone must be one fourth the size of the seal.





The CAE in Cybersecurity Community Logo

The primary CAE in Cybersecurity Community logo consists of two pieces: the icon and the nameplate. While there are different versions of this logo (black and white, all white, full color), the full color logo is the formal and preferred version of the logo. The primary logo should be used on all official documents, publications, and websites.



Font

The font for the CAE in Cybersecurity Community logo is Avenir Next Bold. The text size will depend upon the size of your logo.

Colors

🟦

Blue Shield, Bottom of Gradient
Blue Rim with White Lettering,
Blue Nameplate Lettering:
R3 | G80 | B145
C100 | M76 | Y15 | K2
Hex #035091

🟦

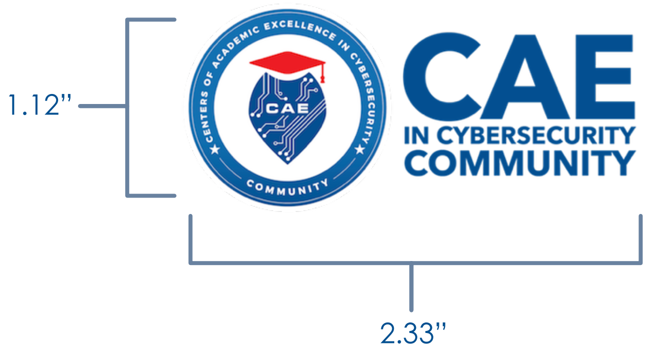
Vertical Gradient Blue Rim with
White Lettering Top:
R19 | G113 | B178
C87.68 | M52.47 | Y4.53 | K0.05
Hex #1371B2

🟥

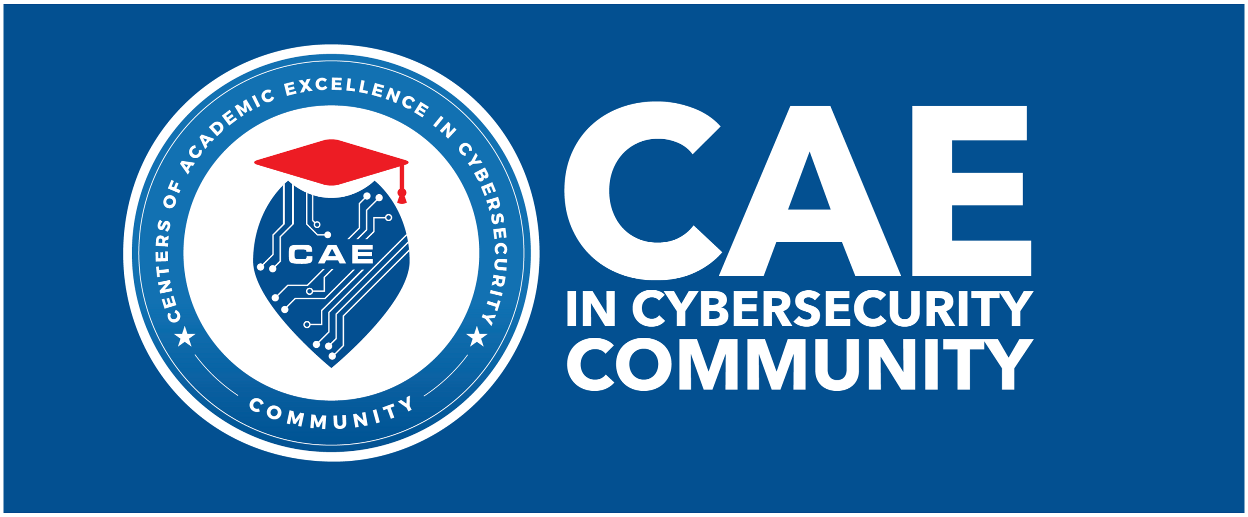
Red Cap:
R236 | G28 | B36
C1 | M99 | Y97 | K0
Hex #EC1C24

Minimum Size

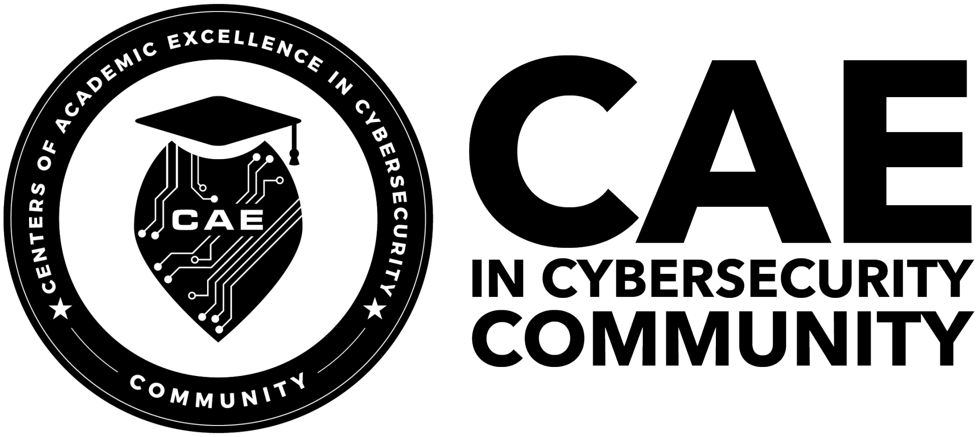
Minimum size for the primary CAE in Cybersecurity logo is 2.33(w)x1.12(h) inches (699x337 pixels). Using this as our minimum size requirement will help others see and distinguish our logo. Any use of the logo smaller that this is often deemed illegible.



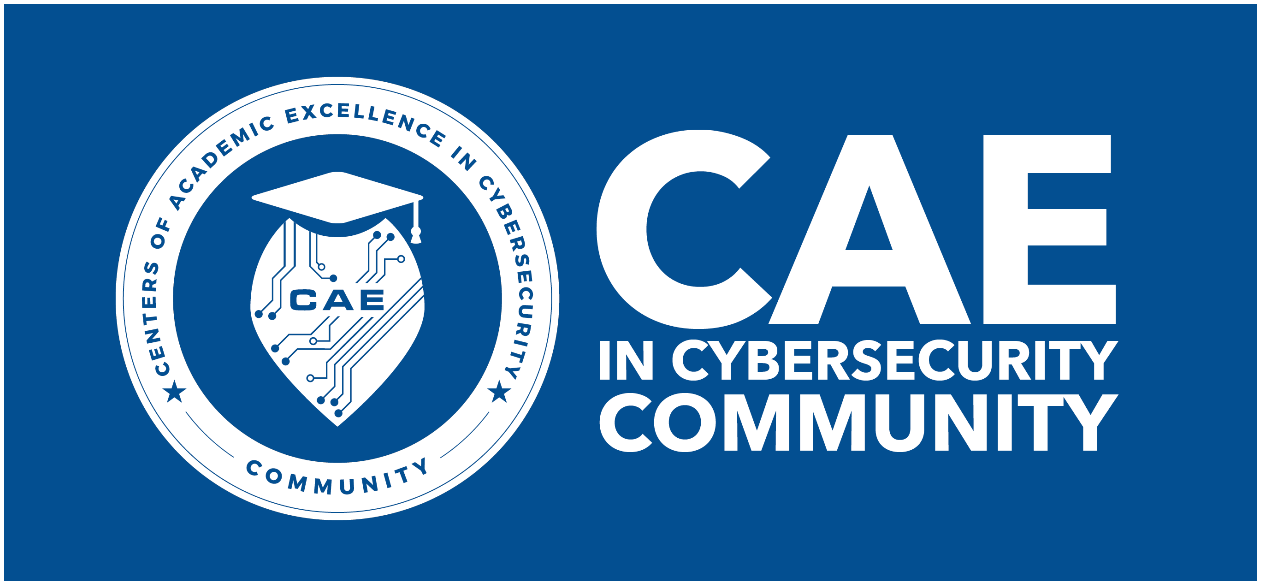
Other Primary Logo Uses



We recognize that sometimes you may want to use a dark background for your marketing purposes. The primary CAE logo is also available with a white nameplate (same color, font, and sizing restrictions apply).



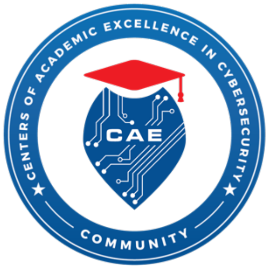
We recognize that sometimes you may want to use a light background for your marketing purposes. The primary CAE logo is also available in black and white (same color, font and sizing restrictions apply).



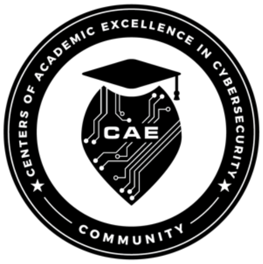
We recognize that sometimes you may want to use a dark background for your marketing purposes. The primary logos are also available in white (same color, font and sizing restrictions apply).

Alternate Logo Usage

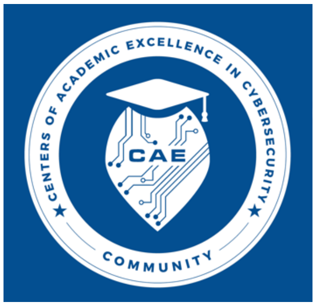
We ask that you generally use the full logo with the nameplate. However, we recognize that sometimes you may only want to use the icon in your design. These icons cannot be altered without official approval from the CAE in Cybersecurity Community Program Manager (info@caecommunity.org).



The CAE in Cybersecurity logo can be used without the nameplate. Use this logo when space is limited or when the other logos present on the design are of a circular shape.



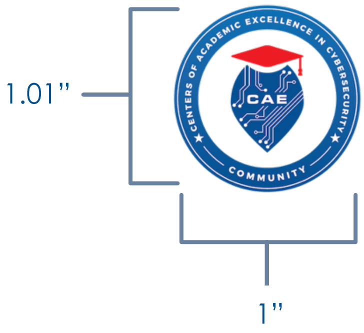
We recognize that some of the designs you will use for your marketing will need differing color schemes. The CAE in Cybersecurity Logo can also be used without the nameplate in black and white.



We recognize that some of the designs you will use for your marketing will need differing color schemes. The CAE in Cybersecurity Logo can also be used without the nameplate in all white.

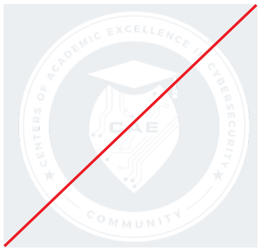
Minimum Icon Size

The minimum size for the primary CAE in Cybersecurity icon is 1”x1.01” or 300x304 pixels. Using this as our minimum size requirement will help others see and distinguish our logo. Any use of the logo smaller that this is often deemed illegible.

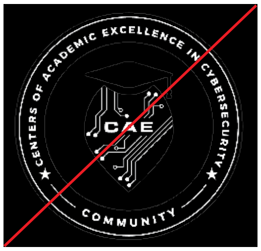


Guidelines for Using the Primary Logo/Icon with Color and Picture Background

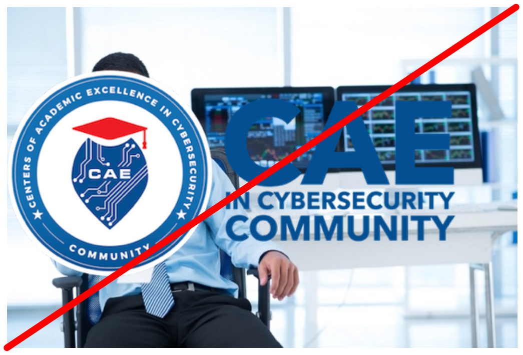
Using color or picture backgrounds can sometimes distort the logo/icon. Therefore, please follow these guidelines when using the primary logos/icons.



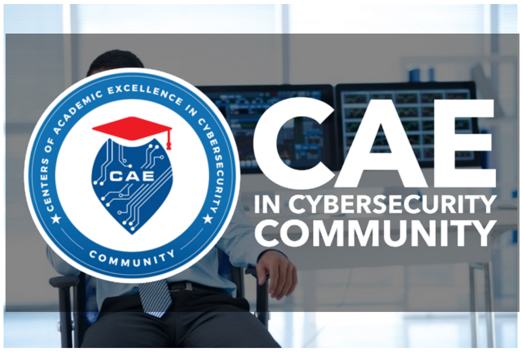
When using our all-white primary logo/icon, do not use the logo/icon against a background that does not have enough of a contrast between the colors. The white logo is not given out unless specifically requested.



When using our black and white primary logo/icon, do not use the logo/icon against a background that does not have enough of a contrast between the colors. The black and white logo is not given out unless specifically requested.

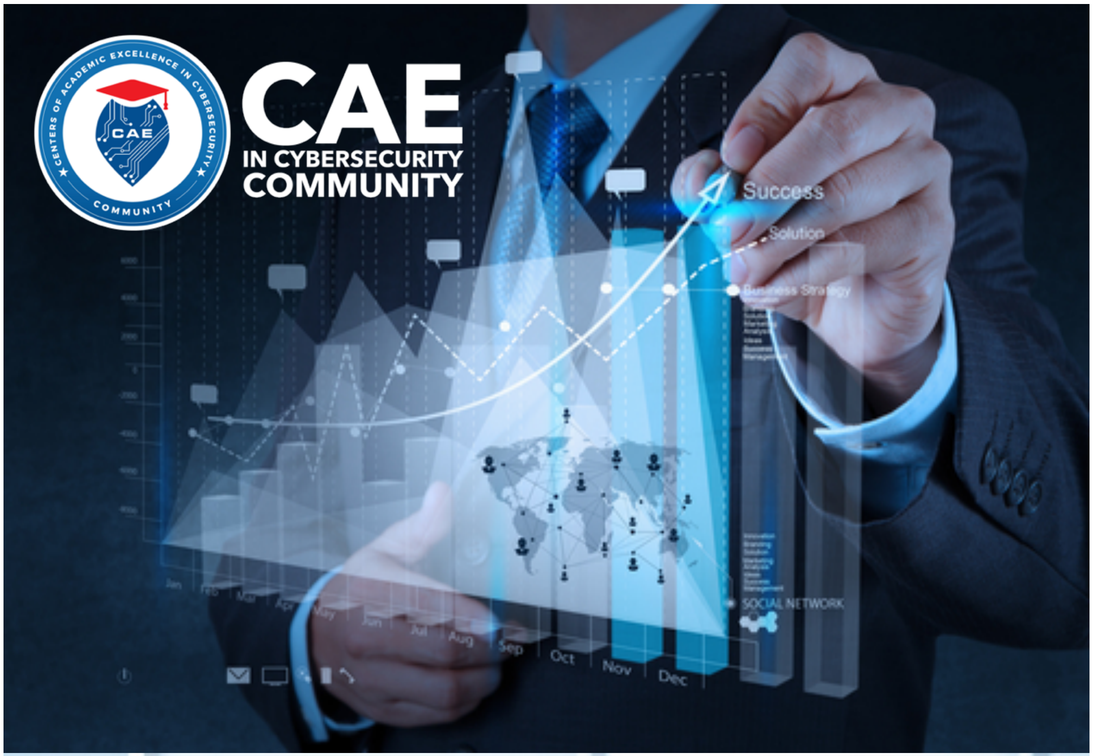


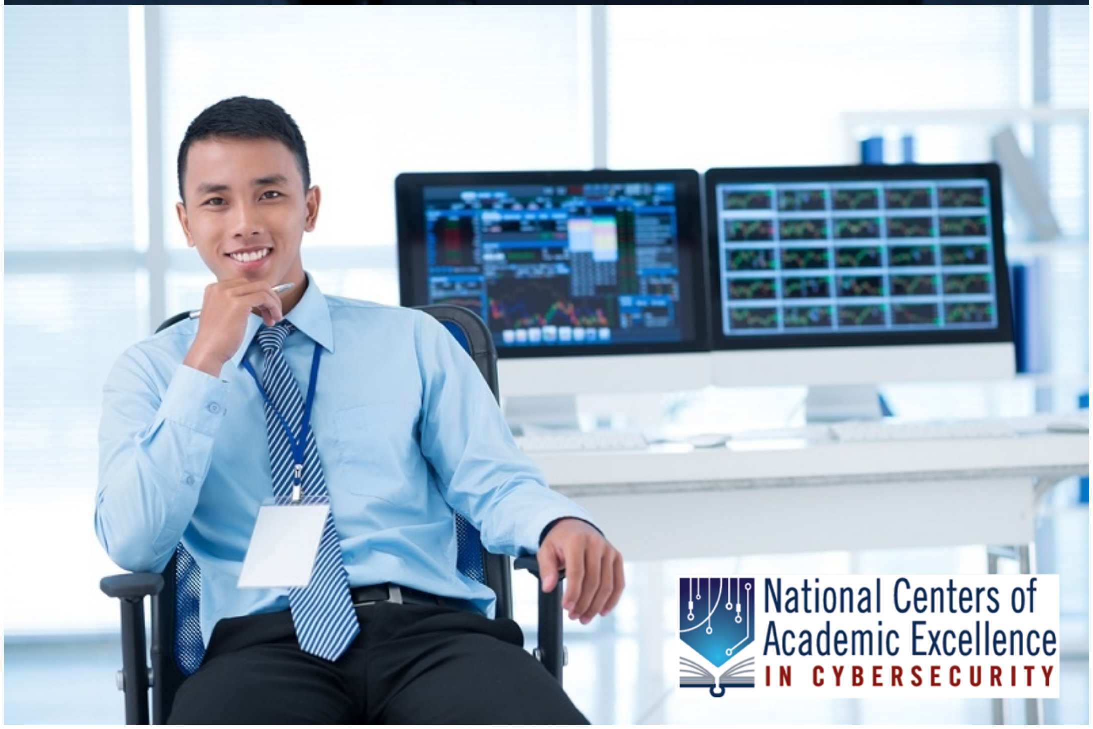
When using our logos/icons, do not use the logo/icon against a background picture that does not have enough of a contrast between the colors. This makes our logo appear illegible.



We recommend placing a dark contrasting background on the picture and using the all-white logo/icon or white text version of the primary logo. This is the best representation of the logo and clearly communicates who we are as a community.

However, there may be times when you can use the logo/icon on a picture without a contrasting backdrop. In the image below, you can clearly distinguish the CAE in Cybersecurity Community logo, which meets the minimum size requirement.





You can also use our black and white logo for any picture or background that is too light for our primary color logo.

Nameplate Rules

While you are allowed to use the icon for your marketing purposes, please do not use the nameplate by itself. The nameplate does not contain any of the stylistic elements that communicate to others our role as Centers of Academic Excellence in Cybersecurity.

Shadowing

We discourage shadowing, but we recognize that sometimes you may want to add a subtle shadow to your design. A light shadowing is acceptable, however heavy shadowing distorts the logo/icon. Please make sure that your shadow does not distort the logo/icon.

Preset, Reflection, Glow, Soft Edges, Bevel, Rotation, and 3D

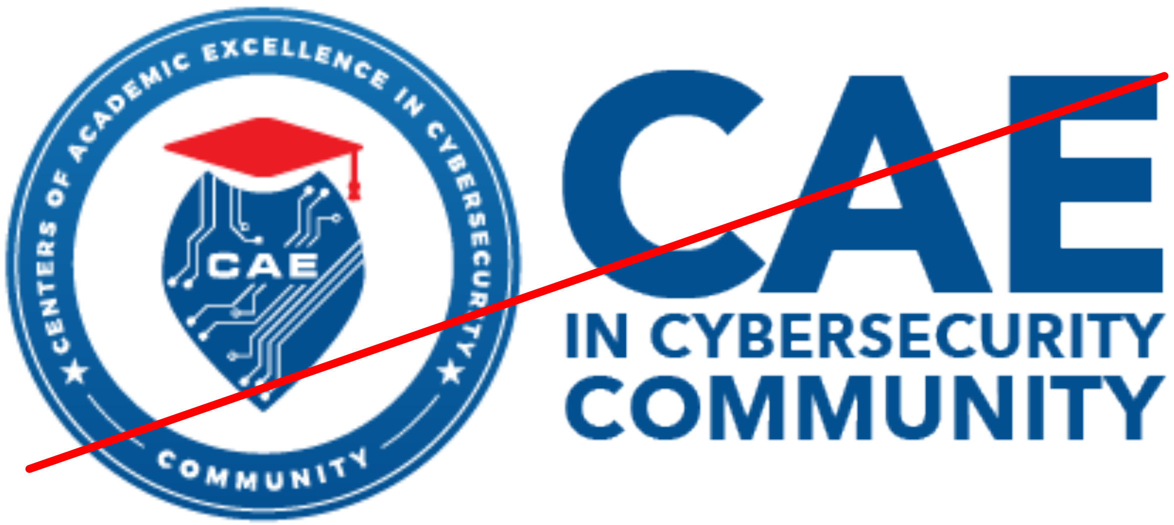
Using tools to distort the logo, such as preset, reflection, glow, soft edges, bevel, rotation, and 3D are not acceptable uses of the logo/icon. These tools distort the logo and make our visual representation sloppy. In addition, adding borders, outlines, etc. can also distort the logo/icon. If in doubt, do not alter the logo/icon.

Blurry, Disfigured, and Distorted Logos

Sometimes you may want to enlarge or decrease the size of the CAE in Cybersecurity Community primary logo/icon. However, during this process the logo/icon can sometimes come out blurry, disfigured, or distorted. Therefore, we ask that if you manipulate the size of your icon/logo and it comes out blurry, disfigured, or distorted, please do not use the logo/icon. At any time, you may request a logo/icon at any size above the minimum and we will be happy to make it for you.

Having a clear, sharp logo/icon will help us as a community communicate a clean, professional outward appearance.

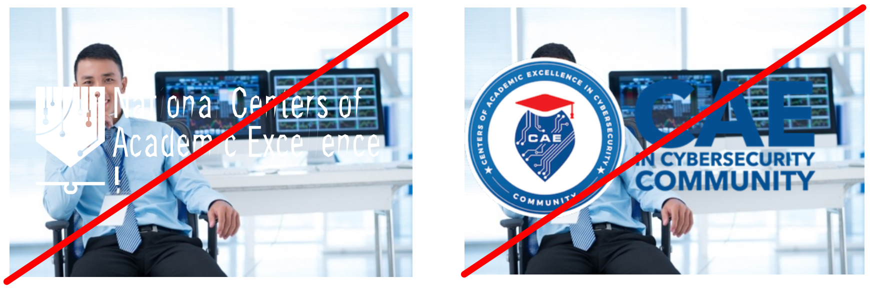
Don'ts:



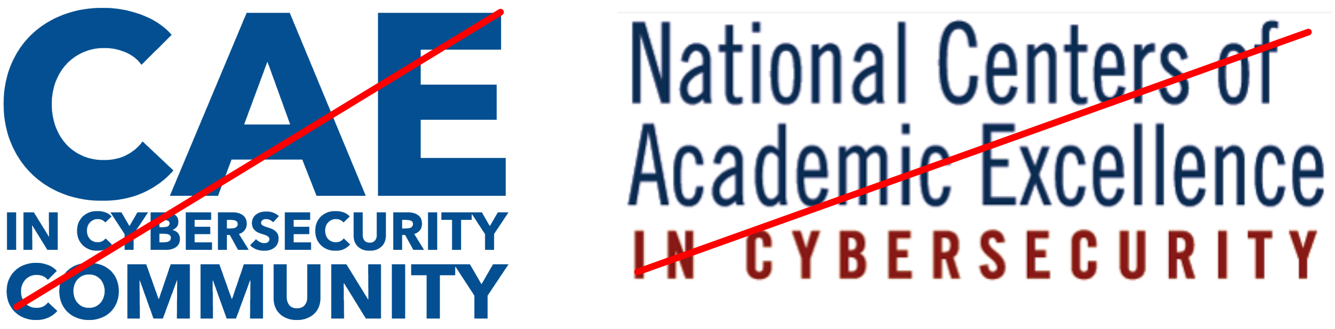
Too Blurry

CAE
IN CYBERSECURIY
COMMUNITY

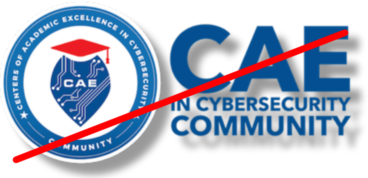
Blurry and Too Small



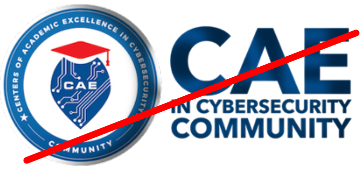
Not Enough Contrast

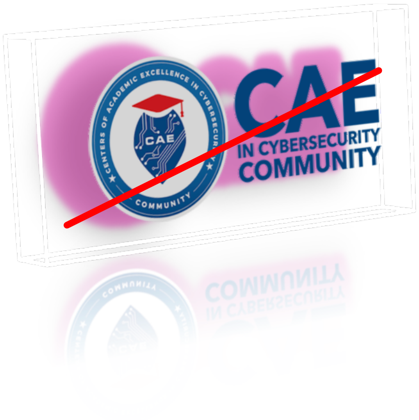


Do not use the Nameplate separate from the Icon

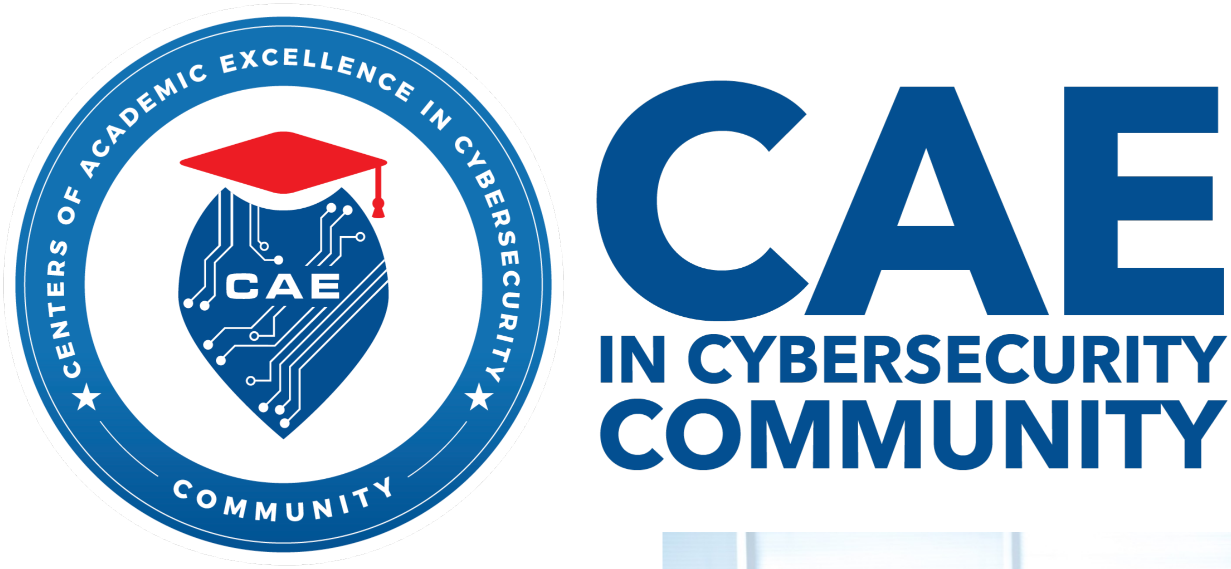


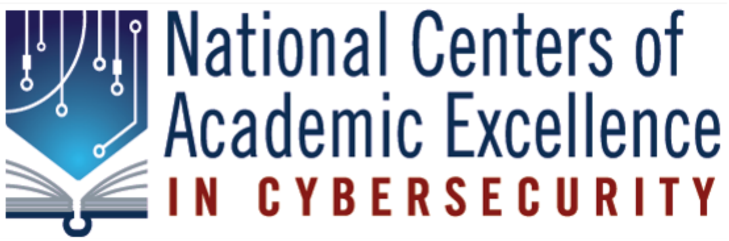
Heavy shadows and 3D effects distort the logo

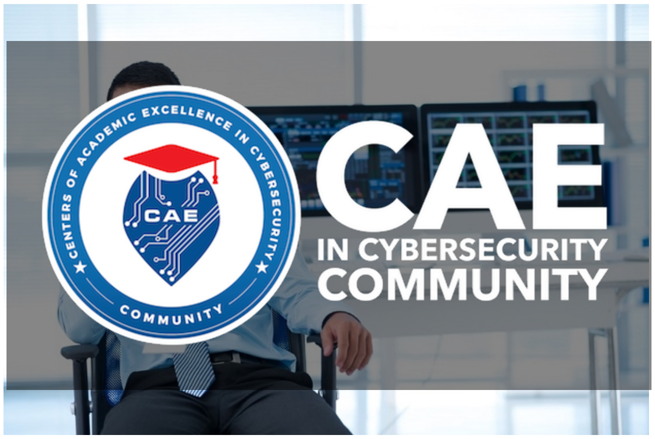




Dos:







Values and Themes

Our visual identity is the result of community feedback, research, and numerous sample designs. Concurrent with this project, the CAE-C team is also in the process of redesigning the Community website. The new website will meet the central themes of the CAE Community, and our logo accomplishes this goal by incorporating: 1) circuitry to represent the cybersecurity industry, 2) a graduation cap to represent our role as educators, 3) a shield and symbolic colors to represent our commitment to producing cybersecurity professionals that will protect the nation's infrastructure, and 4) our full name.

Graphic Standards Oversight

The visual identity program is administered by the CAE in Cybersecurity Community Program Manager and the Web Development Team, which oversee all CAE in Cybersecurity Community publications and graphic design. Visual identity assets will be available for Primary Investigators (PIs) and other approved administrators via the CAECommunity.org website. Policy questions about the rules outlined within this manual should be directed to the CAE in Cybersecurity Community at info@caecommunity.org.

Approval and Usage

This manual outlines the policies and guidelines for using the NCAE-C and CAE Community's visual identity. To ensure that all materials are in compliance with this manual, all communication materials using the visual identity must be approved by the CAE Community Program Manager. To get the CAE in Cybersecurity Logo, you must either be a PI or approved administrator with granted access to the visual identity section of the website. For information about obtaining a CAE in Cybersecurity Community primary logo or icon, please contact info@caecommunity.org. All requests will usually be met within 48-72 hours. You can also contact us at 909-537-7535 for assistance. Please allow at least 48 hours to process this request.

Contact Information

For information about obtaining a CAE in Cybersecurity Community primary logo or icon, please contact info@caecommunity.org. All requests will usually be met within 48-72 hours. You can also contact us at 909-537-7535 for assistance.

The CAE in Cybersecurity Community is under the stewardship of California State University, San Bernardino. Therefore, some of the correspondence between you and the CAE in Cybersecurity Community may come from a @csusb.edu email address.