Excellence within the NCAEs:

Definition and metrics

Executive Summary

The Cyber Academic Engagement Office serves as the strategic nexus between the Department of War (DoW) and the nation's academic institutions, forging an unrivaled cyber workforce and fostering the innovation necessary to ensure the United States maintains a decisive and enduring advantage in the cyber domain. The National Centers of Academic Excellence in Cyber (NCAE) provide a foundation for building a competitive cyber workforce, enacting the collaboration identified in FY26 NDAA Sec 1514 to establish curriculum standards, develop competencies in cybersecurity, promote community outreach, integrate best practices across educational programs, and advance solutions to challenges in addressing educational needs with respect to cyber.

This paper expounds the definition of excellence currently inferred by the NCAE and develops a more concise and agile set of measures to meaningfully evidence excellence to audiences beyond the CAE academic communities.

This paper recommends that the following metrics are vital for evidencing academic excellence in cyber:

- Total number of students studying cyber at each CAE-designated institution (to be used as denominator for other data) and total number graduating from validated Program of Study.
- # of CSA scholars and # of SFS scholars.
- Faculty qualifications, including # of PhDs, Masters, descriptions of recent federal or industry experience, evidence of continuous learning, and descriptions of how faculty members remain up to date with changing threats and emerging technologies.
- A list of all courses taught relating to cyber, and a list of all courses taught that map onto the 8140 DCWF, with evidence of that mapping.
- # of students engaging with internships and apprenticeships.
- # of students participating in competitions.
- A list of faculty members who mentor students for competitions, and their contact details.
- Description of cyber club(s) at the institution.
- Description of local and regional cyber engagements.
- # of graduates who are working within DoW and other federal departments within 6 months of graduation

- A list of grants received by the institution in relation to cyber over the past 5 years, and evidence of delivery and ROI.

Excellence should not be understood as an homogenizing principle, but rather as a foundation upon which the unique qualities of each program might be demonstrated.

The security of the United States is dependent upon the development of a workforce that is mission—ready and able to outperform our adversaries across the entire scope of cyber based on the challenges of today and tomorrow.

1. Introduction

Academic excellence in cyber builds adaptable, independent learners with adversarial mindsets who can evolve to meet current and future threats. By 'cyber', this report adheres to the broad and inclusive approach taken by the DoW in relation to:

- Building, securing, operating, defending, and protecting United States cyber resources.
- Conducting cyber-related intelligence activities.
- Enabling current and future cyber operations.

This approach informs a definition of excellence that encompasses the full spectrum of work and roles within the cyberspace domain.

Excellence is a shared responsibility of the NCAE-C and the CAEO.

2. Defining Excellence

In accordance with the requirements identified in FY26 NDAA Sec 1514, a sustainable ecosystem that provides the DoW with cyber workforce excellence depends upon:

- **Establishing curriculum standards:** Curricula need to be high quality, relevant, and responsive to changing threats and technologies. The amount of time required to design and deliver high quality education resources needs to be radically reduced to enable agility and relevance.
- **Integrating best practices:** Faculty and educators need up-to-date knowledge, training, and resources that will enable pedagogical strategies designed to deliver up-to-date and relevant educational content that matches the current and future needs of the DoW.
- **Developing competencies:** Students graduating from CAEs should possess the competencies needed to meet current workforce standards and the agility to lead future advancements. Extra-curricular activities and experiential learning are central to building real-world abilities.
- **Promoting community outreach:** Academic institutions should contribute to the security of their communities and excellence in cyber should strengthen the cyber posture of the regional civic infrastructure.
- **Advancing solutions to challenges in addressing educational needs with respect to cyber:** Excellence requires an ongoing commitment at an institutional level to continuously to evolve and improve.

3. Stakeholder perspectives

The NCAEs have three main categories of stakeholder. The first two of these stakeholder groups have actively participated in the development of our understanding of excellence.

- **Faculty, institutions and teaching community** deliver teaching and research. In 2025, faculty, educators and program leads worked collaboratively to agree a definition of excellence as: "*a dynamic quality defined by three core pillars:*
    - *rigor and relevance in teaching and scholarship;*
    - *the cultivation of cyber talent prepared for DoW work roles; and*
    - *a commitment to meaningful, continuous improvement that forges immediate workforce readiness and sustained leadership in defense of the nation."*

- **The DoW** define the cyber work force through the DCWF 8140, a framework that clearly identifies the knowledge, skills and abilities associated with each cyber work role and which categorizes three levels of achievement.

- While **students** can informally evaluate courses and instructors, more comprehensive opportunities to evaluate excellence are not currently in place. This might provide an opportunity to work with graduates and alumni in the future.

4. Current measures of excellence

Excellence relates to immediate, short-term, medium-term, and longer-term goals. In a rapidly changing workplace, excellence risks expanding into a portmanteau term that struggles to contain both the qualities necessary to do a job now and the need to rapidly adapt and pivot to the changing technologies, threats and workplace practices of the near and longer-term future.

Previously the academic communities within the NCAE have defined excellence in relation to rigorous analyses of curricula and educational standards. This process has raised the following challenges:

- Data collection is retrospective, describing courses that have been taught rather than anticipating courses that will be taught. Designation data can be up to 5 years out of date prior to redesignation, and this is in tension with the 8140 which is reviewed and updated in 12-week cycles.
- Validation of programs of studies requires that they have been taught for at least 3 years if they are to be considered as excellent. This reduces agility and precludes courses that have been designed to

respond to emerging threats and evolving technologies. This contributes to the lag between the DoW need and the educational response.

- To be designated as a Center of Academic Excellence in Cyber in one of the existing designation categories (Cyber Defense, Cyber Operations, Research, or Cyber AI), institutions are required to complete a lengthy administrative process (see Appendix 1) that is time-consuming for applicants and requires significant input from peer mentors. Furthermore, the diversity of data types and the heavy reliance on pdfs limit the ability for users to systematically search for usable metrics to evidence excellence and demonstrate ROI.
- The DoW has had limited input into knowledge units and required metrics, although some designation types require crosswalks to be evidenced between their knowledge units and the DCWF.

In summary, current measures of excellence focus on proving rather than improving, with a reliance on accounting over accountability. The system is bureaucratic and slow. To foster excellence, we must move beyond simple accounting and build a system of accountability where data is the primary tool for learning, adaptation, and continuous improvement.

5. An improved information management system

Excellence should not be an abstract concept, but an evidenced foundation for all institutions designated as Centers of Academic Excellence in Cyber. Measures of excellence also need to be timely, agile and relevant. An effective information management system will empower users through an intuitive, self-service interface that minimizes the need for training and support. It will streamline data input, reduce administrative burden and focus on accountability rather than mere process. An effective system will provide robust reporting and analytics, enabling the efficient retrieval of data to clearly demonstrate return on investment and measure outputs. Core to its design will be a commitment to security, ensuring full compliance with data protection regulations. Finally, it will serve as a central hub for seamless communication and collaboration with points of contact and external institutions. To gain comprehensive understanding of student success, longitudinal data gathering will also be needed.

Therefore, the CAEO requires the following to effectively and meaningfully evidence excellence to our DoW stakeholders. the following data should be collected from each institution designating, or designated, as a Center of Academic Excellence in Cyber. Importantly, the majority of these data are already supplied through the mandatory Annual Reporting system for designated schools. We require that all these data fields should be reviewed and updated at least once a year as part of the designation requirements.

Establishing curriculum standards
1. A list of all courses taught relating to cyber, identification of those that map onto the DCWF 8140, and evidence of that mapping.
Integrating best practices
2. Faculty qualifications, including # of PhDs, Masters, descriptions of recent federal or industry experience, evidence of continuous learning, and descriptions of how faculty members remain up-to-date with changing threats and emerging technologies.
3. A list of faculty members who mentor students for competitions, and their contact details.
4. A list of advisory board members.
5. Description of cyber club(s) at the institution.
Developing competencies
6. Total number of students studying cyber (to serve as denominator for other statistics)
7. # of CSA scholars and # of SFS scholars.
8. # of students engaging with internships and apprenticeships.
9. # of students participating in competitions.
10. Examples of students' achievements mapped against DCWF 8140 criteria.
11. # of students graduating cyber courses each year.
12. # of graduates who are working within DoW and other federal departments within 6 months of graduation (and denominator of how many students graduated from cyber courses in the past 6 months)
Promoting community outreach
13. Description of local cyber engagements including, for example, K12 outreach, engagement in regional security centers, engagement with local public facilities including libraries, firehouses, schools, libraries etc.
Advancing solutions to challenges in addressing educational needs with respect to cyber
14. A list of grants received by the institution in relation to cyber over the past 5 years, and evidence of delivery and ROIU.

6. Conclusions

The Department of War faces a critical choice: proactive investment in its cyber workforce or the costly consequences of reactive failure. An undertrained force is condemned to a perpetual state of reaction, incapable of seizing the initiative from adversaries or harnessing emerging technologies. Investing in educational excellence is central to gaining and maintaining advantage.

Formalizing the definition of what is meant by excellence in relation to the National Centers of Academic Excellence in Cybersecurity establishes a common core of requirements for all institutions. This is not intended to describe everything an institution does, because institutions should aim to develop their own unique strengths and specialized capabilities. Excellence establishes the benchmark upon which additional provision will be built.

Guided by the CAE community's definition and the mandates of FY26 NDAA Sec. 1514, targeted data will be collected to measure this standard. This data will provide clear evidence of performance at the student, faculty, and institutional levels. The resulting insights will directly strengthen the DoW's cyber ecosystem by:

- Identifying the specific location and capabilities of graduating talent.
- Increasing the agility and mission-relevance of academic cyber curricula.
- Driving meaningful engagement in extracurricular and community-based activities.

Ultimately, this initiative strengthens national security at local and regional levels while also forging robust talent pipelines directly into the Department of War.

Appendix 1: Existing data gathered to designate as a Center of Academic Excellence

Dimension	Description	Measures
Institutional	Yes/no measures	Yes/no measures: - Regionally accredited - Leadership support - Institution has cybersecurity posture - Department has continuous improvement plan - Department has formal relationships with career services platform (e.g. LinkedIn, Handshake etc). - Mandated 'Center' for cybersecurity with dedicated administrative lead.
Advisory Board	Yes/no measures	- Advisory board
Program of Study	Mainly pdfs	- Course syllabus and program learning outcomes - Curriculum mapping to CAE-defined KUs - Assessment indicators - Examples of lab exercises - Cross walk between KUs and 3 DCWF work roles - Outreach activities to community
Faculty		- Faculty resumes - Evidence of promotion process - Faculty attendance at CAE annual symposium
Students		- Enrollment figures - Institutional letter - Transcripts - Certificates - Examples of work - Competency statements mapped to DCWF - Examples of engagement in ethical education - Every student has an opportunity to participate in at least one competition - Every student has an opportunity to participate in at least one cyber range - Every student completes at least one mandatory work-integrated learning experience (internships, co-op, practicum)