

**Federal Cybersecurity Workforce Expansion Act**  
**Section-by-Section Summary**  
Senators Hassan and Cornyn

This bill would augment cybersecurity workforce development pathways, by adding 2 new programs: one to establish a cybersecurity apprenticeship program in the Cybersecurity and Infrastructure Security Agency (CISA); and the other to establish a pilot program within the Department of Veterans Affairs to give cybersecurity training to veterans. These cybersecurity workforce programs are based on a recommendation from the Solarium Commission.

Section 1 states that the short title of the bill is the “Federal Cybersecurity Workforce Expansion Act.”

Section 2 includes findings identifying the need for additional federal cybersecurity professionals.

Section 3 inserts a new section into the Homeland Security Act of 2002 to create a cybersecurity apprenticeship program within CISA at DHS.

Subsection 2218(a) defines many different workforce, education, and apprenticeship related terms. We are aware of ongoing efforts within the Committee on Health, Education, Labor, and Pensions to better define apprenticeship related terms, and we have committed to referencing or mirroring any updates to the appropriate terms before passage, if needed.

Subsection 2218(b) gives CISA up to 2 years to establish at least one apprenticeship program. CISA requested sufficient lead time for setting up the program, so it would be effective and not nearsighted because it was rushed to creation.

Subsection 2218(c) requires the apprenticeship program to:

- Lead directly to employment at CISA or as a contractor hired by CISA, ensuring the program actually helps CISA build their workforce pipeline;
- Focus on the skills needed to meet CISA’s cybersecurity work needs; and
- Be a registered apprenticeship approved by the Office of Apprenticeship of the Department of Labor.

Subsection 2218(d) requires CISA to consult with the Departments of Labor and Defense, the National Institute of Standards and Technology (NIST), the National Science Foundation (NSF), and the Office of Personnel Management (OPM) to leverage existing resources, knowledge, and experience from across the federal government.

Subsection 2218(e) gives CISA the option to enter into contracts or cooperative agreements with eligible entities to help implement the apprenticeship program. Eligible entities should have knowledge of cybersecurity workforce development and experience with implementing or supporting apprenticeship programs with positive outcomes.

Subsection 2218(f) gives CISA flexibility for requirements for eligible entities seeking a contract or cooperative agreement.

Subsection 2218(g) allows CISA to prioritize eligible entities that:

- Are members of an industry or sector partnership;
- Have experience providing instruction for cybersecurity or related apprenticeships;
- Help veterans and members of the armed forces transition to civilian jobs; or
- Plans to work with a State agency on the apprenticeship or with an entity that receives State funding.

Subsection 2218(h) requires CISA to provide technical assistance to eligible entities to leverage existing federal programs and resources.

Subsection 2218(i) refers to the hiring flexibility provided in the Border Patrol Agent Pay Reform Act of 2014 for hiring cybersecurity positions, and would allow graduates from CISA's apprenticeship program to be hired using that authority.

Subsection 2218(j) requires CISA to report to Congress every 2 years on the activities carried out to implement an apprenticeship program by CISA and any entities that CISA worked with, along with an assessment of the results achieved by the apprenticeship program.

Subsection 2218(k) requires CISA to submit annual reports to Congress and the Secretary of Labor on the effectiveness of the apprenticeship based on standard metrics laid out in statute.

Subsection 2218(l) authorizes such sums as necessary to implement the apprenticeship.

Section 4 establishes a pilot cybersecurity training program within the Department of Veterans Affairs (VA).

Subsection (a) defines "eligible individuals" as members of the Armed Forces transitioning to civilian life or a veteran, "portable credentials" as a documented award that shows an individual has achieved specific learning outcomes and "work-based learning" as the definition given in the Carl D. Perkins Career and Technical Education Act of 2006.

Subsection (b) directs the VA to establish the pilot program within 1 year.

Subsection (c) requires that the pilot program incorporate virtual coursework/training, hands-on labs and assessment, and Federal work-based learning opportunities, and that the pilot program give graduates from the program portable credentials.

Subsection (d) requires the program to align with the National Initiative for Cybersecurity Education Workforce Framework (NICE framework).

Subsection (e) requires the VA to coordinate with the Departments of Homeland Security, Defense, and Labor, the National Institute of Standards and Technology (NIST), and the Office of Personnel Management (OPM) to leverage existing resources and platforms from across the Federal government and to identify or create work-based learning opportunities.

Subsection (f) requires the VA to provide or procure the resources necessary to ensure that the pilot program can accommodate increased participation from veterans and transitioning service members, ensure that they remain engaged, and successfully connect graduates to job opportunities within the Federal government.

Section 5 extends the requirement for OPM to conduct an annual agency-wide cybersecurity position survey and report through 2025.