



For Immediate Release

Contact:

AGB: Morgan Alexander

media@AGB.org

202-776-0853

ISA: Larry Clinton

lclinton@isalliance.org

202-236-0001

EDUCATION AND SECURITY ORGANIZATIONS UNITE TO SUPPORT
CYBERSECURITY ACADEMY

The Association of Governing Boards of Universities and Colleges (AGB) and the Internet Security Alliance (ISA) are making a unified appeal to Congress and the Biden administration to create a national, virtual cybersecurity academy to address the nation's long-standing cybersecurity workforce gap.

In a joint letter ([link](#)) to the House and Senate Appropriations Committees, AGB President and CEO Henry Stoever and ISA President and CEO Larry Clinton state, "The nation faces a severe, and growing, cyber threat from multiple adversaries. Funding a virtual cybersecurity academy is the only way to create a workforce to combat these threats."

The letter argues that what the United States "traditionally has referred to as a 'workforce gap' is really a lack of adequate national defense mobilization. National defense in the digital age requires more than an adequately trained military—the United States needs trained cyber defenders throughout the government as well as the private sector. The reality is that the entire nation, both the public and private sectors, is under cybersecurity attack from all manner of adversaries, including nation-states such as China, Iran, North Korea, and others. The United States simply doesn't have enough people, not just in the Department of Defense but nationwide, to put up an adequate defense."

Stoever acknowledges that although a wide number of excellent cybersecurity workforce programs have been established in recent years, it has become clear that this patchwork approach is not fulfilling the nation's urgent cybersecurity workforce/defense mobilization needs. "The country has over 700,000 cybersecurity job openings going unfilled," he said. "That gap has [increased 29 percent from last year](#), and it won't slow down. The country needs to provide more training and opportunity, as it does with other national priorities."

The joint letter calls for immediate funding of a program—initiated in last year's National Defense Authorization Act—that would create a digital academy run by the Department of

Defense. Stoever and Clinton suggest an initial appropriation of \$200,000 a year, ramping up over five years to an annual appropriation of \$1 million, which would support an influx of 10,000 new students into the cybersecurity field.

Clinton highlights that the federal government is currently spending over \$60 billion on cybersecurity. “The very first billion the nation spends on this issue should be for the cybersecurity academy because it’s axiomatic that none of the nation’s other programs can work properly without enough adequately trained people to implement them,” he said. “The regulations can’t work. The technology can’t work. The frameworks can’t work. Nothing works without the people. This should, finally after 20 years, be the nation’s top priority.”

The joint letter concludes, “This is, at heart, an economics issue of supply and demand. To resolve it, the nation needs to stimulate the supply, i.e., the number of people who will go into cybersecurity. The academy would solve this problem the same way the United States solves other national defense workforce problems, by providing free tuition in return for a specified term of government service.”

About AGB

The Association of Governing Boards of Universities and Colleges (AGB) is the premier membership organization that strengthens higher education governing boards and the strategic roles they serve within their organizations. Through our vast library of resources, educational events, and consulting services, and with more than 100 years of experience, we empower 40,000 AGB members from more than 2,000 institutions and foundations to navigate complex issues, implement leading practices, streamline operations, and govern with confidence. AGB is the trusted resource for board members, chief executives, and key administrators on higher education governance and leadership. Learn more at AGB.org.

About ISA

The mission of the Internet Security Alliance (ISA) is to integrate advanced technology with economics and public policy to promote a sustainably secure cyber system. The ISA board consists of cyber leaders (typically chief information security officers) from virtually every critical industry sector. For more than 20 years, ISA has created a comprehensive theory and practice for cybersecurity covering both enterprise risk management and government policy. ISA’s consensus principles and practices, developed in collaboration with NACD and the World Economic Forum, are the foundation of this program and are contained in ISA’s numerous Cyber-Risk Handbooks.

The ISA board has created a companion book *Cybersecurity for Business* (with a foreword from NACD president and CEO Peter Gleason) that translates the board level principles into roles and practices for a corporation’s management team.

ISA has also defined a new approach to public policy on cybersecurity in its new book, *Fixing American Cybersecurity: Creating a Strategic Public Private Partnership*. Many of the proposals ISA makes in *Fixing American Cybersecurity* are integrated into the new National Cybersecurity Strategy recently released by President Biden.

More information regarding ISA can be found at isalliance.org.



Dear Congressional Members of the House and Senate Appropriations Committees:

We are writing to urge the House and Senate Appropriations Committees in the fiscal year (FY) 2024 appropriations bill to include \$200 million for the Department of Defense Cyber and Digital Service Academy (the Academy) that was authorized in the FY 2023 National Defense Authorization Act, with greater levels of funding included year over year for five years. The nation faces a severe, and growing, cyber threat from multiple adversaries. Funding a virtual cybersecurity academy is the only way to create a workforce to combat these threats.

Funding the Academy would acknowledge that what the United States traditionally has referred to as a “workforce gap” is really a lack of adequate national defense mobilization. National defense in the digital age requires more than an adequately trained military—the United States needs trained cyber defenders throughout the government as well as the private sector. The reality is that the entire nation, both the public and private sectors, is under cybersecurity attack from all manner of adversaries, including nation-states such as China, Iran, North Korea, and others. The United States simply doesn’t have enough people, not just in the Department of Defense but nationwide, to put up an adequate defense.

Although a wide number of excellent cybersecurity workforce programs have been established in recent years, it has become clear that this patchwork approach is not fulfilling the nation’s urgent cybersecurity workforce/defense mobilization needs. In fact, the size of the cyber workforce gap continues to grow. Current estimates indicate that over 700,000 cybersecurity job openings in the United States are unfilled. Additionally, according to recent research by Microsoft, the gap has increased 29 percent in the last year, doubling the rate of growth from 2018 and 2019. The virtual academy approach would enable the United States to use modern digital techniques to link the current programs, better leverage faculty, and reach a vast new supply of potential cyber trainees. We estimate an eventual annual appropriation of \$1 billion (phased in at \$200 million a year) would enable a fully functioning academy attracting up to 10,000 new candidates a year. This program would eliminate the full federal workforce gap in less than four years, and then go on to support the rest of the nation’s cyber defense needs. Without such an academy to address the issue at scale, none of the other cybersecurity programs or the related regulations, frameworks, and technologies the United States is funding can be effective because the nation does not have an adequately trained workforce to implement them. The first billion dollars the nation spends on cybersecurity should fund the virtual academy.

Unlike many cybersecurity issues, the defense mobilization/workforce gap is an issue that can be *solved*, which is a word not often used in cybersecurity. The nation does know how to train a sophisticated workforce. This is, at heart, an economics issue of supply and demand. To resolve it, the nation needs to stimulate the supply, i.e., the number of people who will go into cybersecurity. The academy would solve this problem the same way the United States solves

other national defense workforce problems, by providing free tuition in return for a specified term of government service.

We appreciate your attention to this pressing matter and urge your utmost consideration.



Larry Clinton
President and CEO
Internet Security Alliance



Henry Stoeber
President and CEO
Association of Governing Boards of
Universities and Colleges