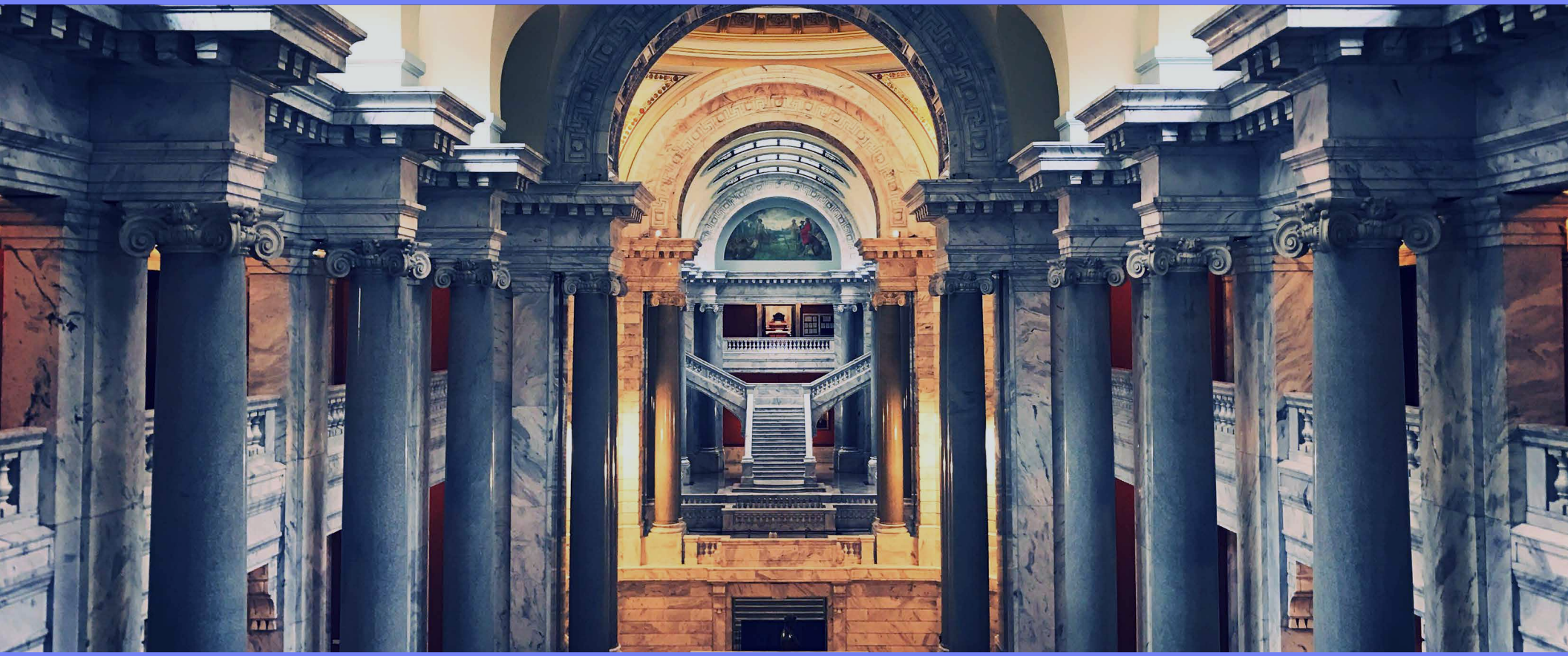
KENTUCKY CYBERSECURITY INDUSTRY STUDY | JUNE 2017



This study was prepared under contract with the Commonwealth of Kentucky, with financial support from the Office of Economic Adjustment, Department of Defense. The content reflects the views of the Commonwealth of Kentucky, and does not necessarily reflect the views of the Office of Economic Adjustment.

simon everett
an analytic design firm

EXECUTIVE SUMMARY

In September 2016, the Commonwealth of Kentucky commissioned a team led by Simon Everett, Ltd., and its partner kglobal, LLC, to conduct the first-ever statewide study of cybersecurity in Kentucky. This study was made possible by a grant awarded to the Kentucky Commission on Military Affairs (KCMA) by the Department of Defense (DoD) Office of Economic Adjustment (OEA). Through grants like this one, OEA helps communities adjust to the economic impacts of fluctuations in defense spending.

Through independent research, stakeholder interviews, and an industry survey, our team sought to understand, assess, and make actionable recommendations to improve the state of cybersecurity in the Commonwealth. In particular, the study is designed to help Kentucky's policymakers devise strategies to meet three objectives:

- make the defense industrial base more resilient by helping defense companies better assess opportunities for growth and diversification in the cybersecurity sector;
- strengthen the economy by creating an environment conducive to the growth of the cybersecurity industry; and
- protect critical infrastructure by empowering government agencies, businesses, and citizens to create a healthy cybersecurity ecosystem.

The study addresses ten topic areas, as shown on the right. In this executive summary, we will recap the study's major findings and key recommendations.

ECONOMIC IMPACT

ECONOMIC INCENTIVES

WORKFORCE

EDUCATION

GOVERNANCE

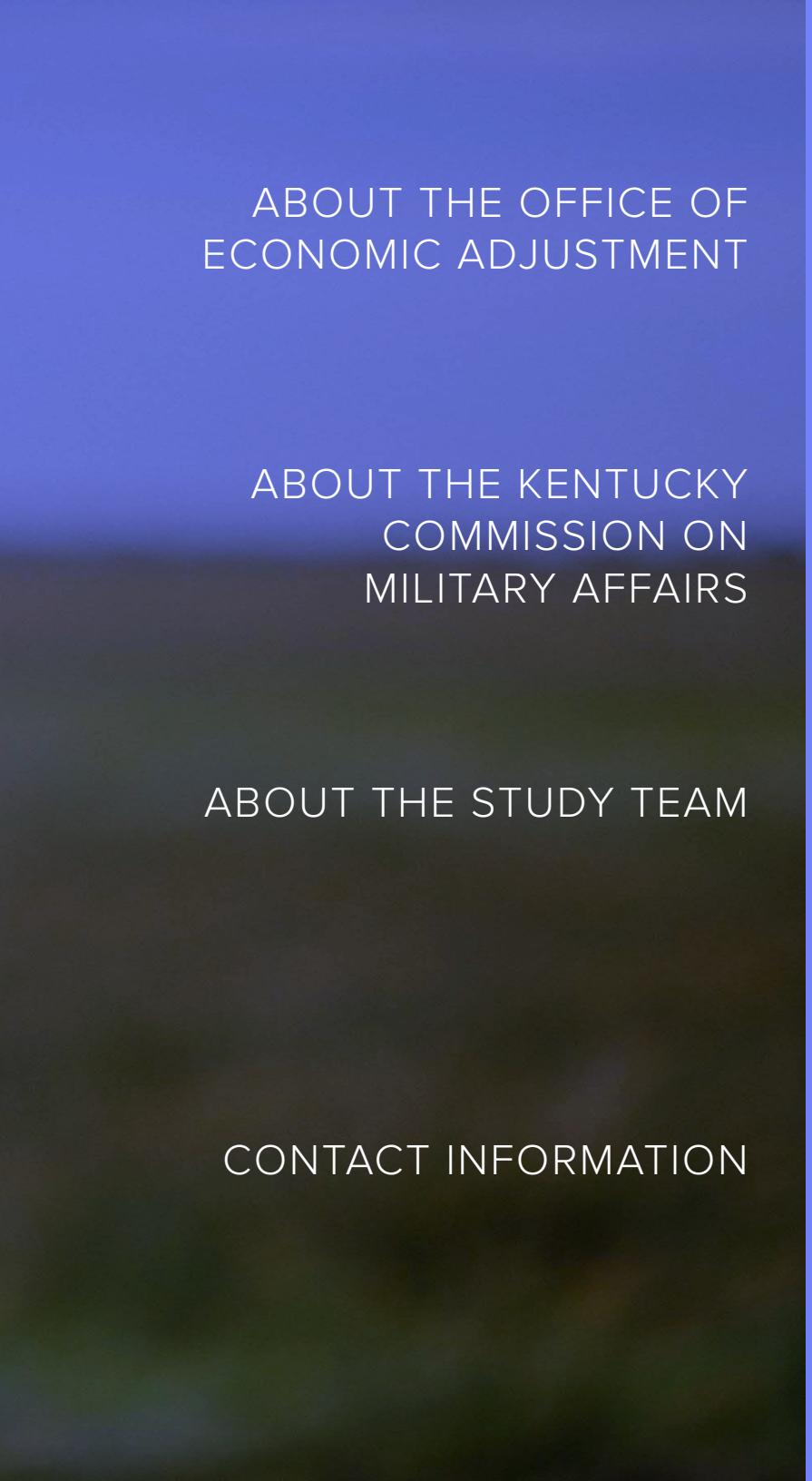
DEFENSE PARTNERSHIPS + EMERGENCY MANAGEMENT

CAPABILITIES + AWARENESS

RISK MANAGEMENT

PRIVACY

CYBERSECURITY INITIATIVE



ABOUT THE OFFICE OF ECONOMIC ADJUSTMENT

OEA is the Department of Defense's field organization responsible for supporting state and local government's response to defense program changes, such as base closures, base restructuring or realignment, growth issues surrounding compatible land and air use for military bases and communities, and other issues that can impact the economy of a region.

ABOUT THE KENTUCKY COMMISSION ON MILITARY AFFAIRS

The Kentucky Commission on Military Affairs (KCMA) is an independent agency attached to the Office of the Governor. It is the lead advocate for military installations and the related defense economy in Kentucky. KCMA has directly managed Base Re-alignment and Closure (BRAC), set conditions for economic growth near Kentucky military installations, and provided insight to all levels of government regarding the military and veterans.

ABOUT THE STUDY TEAM

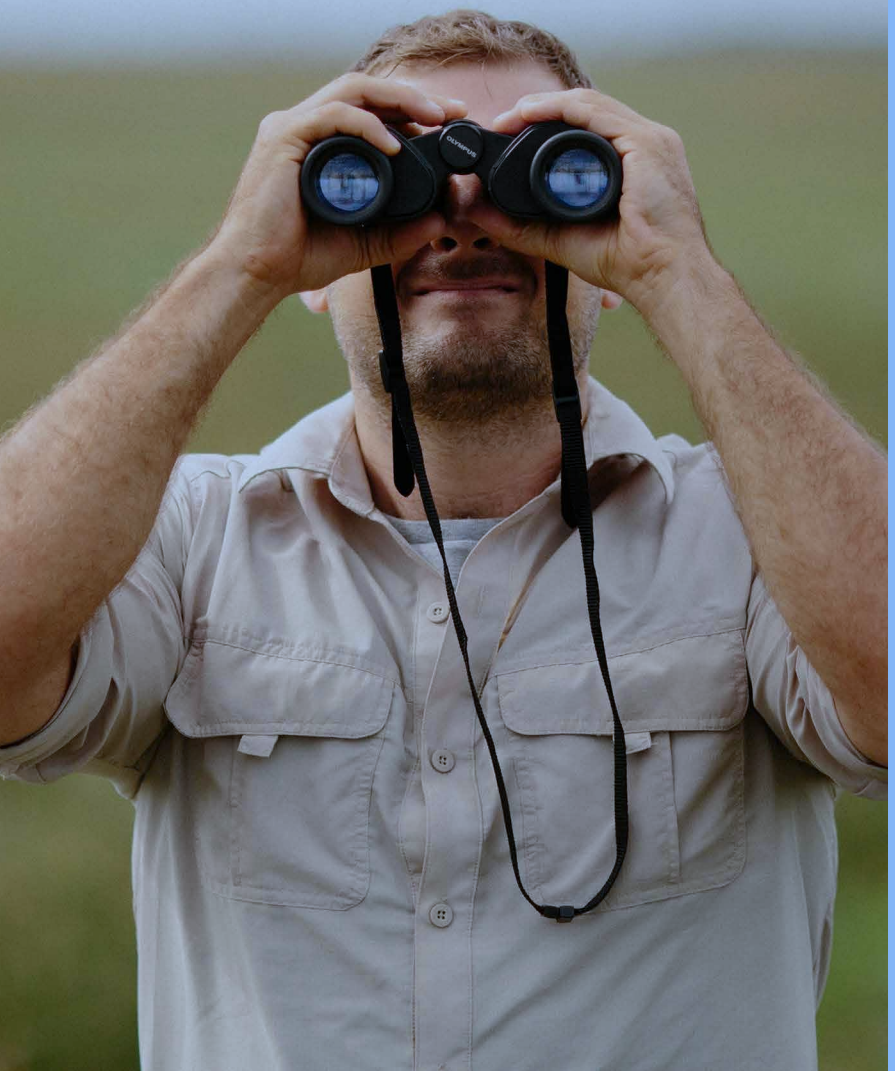
Simon Everett is an analytic design firm that conducts objective research and analysis to support strategic planning efforts on issues like defense diversification and cybersecurity. kglobal is a strategy and communications firm that works with public and private sector clients on a range of economic development programs. Together, we have worked in four states and with more than 20 individual defense companies under OEA-supported initiatives to strengthen economic and workforce resilience.

CONTACT INFORMATION

For more information about this study, please contact:

- Simon Everett // inquiries@simon-everett.com
- Kentucky Commission on Military Affairs // 502.564.2611, extension 302

KEY FINDINGS



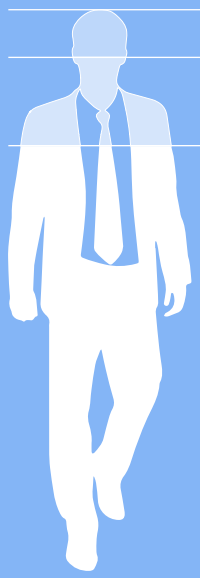
Although it represents a small portion of the economy, Kentucky's cybersecurity sector is filled with opportunity. Cybersecurity workers earn more than the average worker, and cybersecurity companies can spur innovation, investment, and additional economic activity. Moreover, the Commonwealth has key infrastructure in place to enable the growth of the sector: an educational system with broad-based computer science programs, advanced research and development institutions, tax incentive programs for business attraction and retention, and a growing information technology hub in Louisville.

Kentucky has also taken significant strides in bolstering the state's cybersecurity posture. It has partially centralized the state government's information technology infrastructure within the Commonwealth Office of Technology (COT); the Kentucky Office of Homeland Security (KOHS) is planning to increase its focus on cybersecurity information sharing; and the Kentucky Army National Guard (KYARNG) is a leader among its peers in the cybersecurity field. Moreover, the state government has adopted two laws to help protect the data of Kentucky's citizens.

The Kentucky Cybersecurity Industry Study yielded dozens of insights into the cybersecurity landscape in the Commonwealth, covering a range of economic and security issues. In this section, we highlight 22 of the most salient findings.

The cybersecurity industry has an estimated economic impact of $730,277,977 in Kentucky.

When compared against Kentucky's Gross State Product for 2015, this figure represents 0.37% of the total. The bulk of the cybersecurity industry's impact (92%) results from economic effects induced by the spending of cybersecurity workers, rather than direct (6%) or indirect (2%) effects.



9,516 approximate total

9,383 are performing cybersecurity functions

8,825 are supporting the internal cybersecurity needs of companies in non-cybersecurity sectors

1

$730,277,977

ECONOMIC IMPACT OF THE CYBERSECURITY SECTOR

2

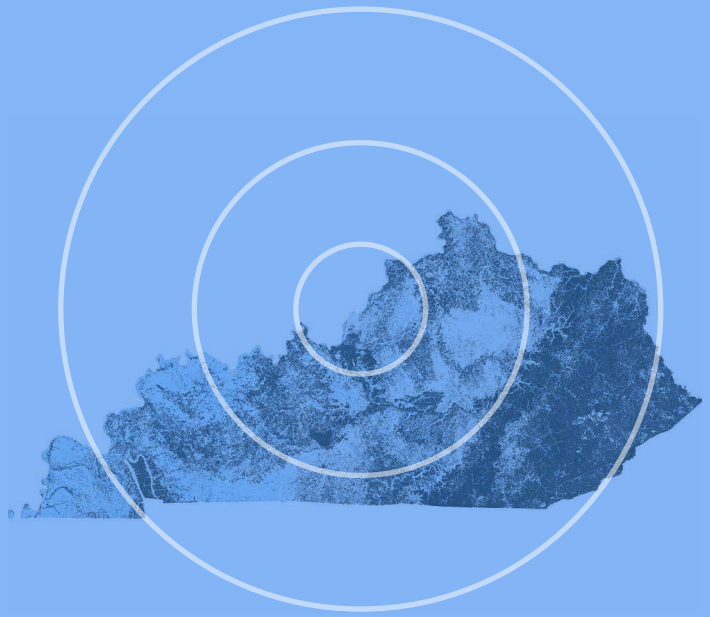
Kentucky's cybersecurity sector is small.

There are 54 companies in Kentucky that sell cybersecurity goods and services, but only a handful are "pure play" cybersecurity companies. Most are managed services companies that provide cybersecurity as part of a larger information technology capability suite. Kentucky lacks a critical mass of disruptive, cutting-edge cybersecurity companies that generate the buzz required to attract innovators and investors.

3

Most of Kentucky's cybersecurity workers do not work at cybersecurity companies.

Approximately 9,516 people work in Kentucky's cybersecurity sector, 9,383 of whom are performing cybersecurity functions. Of that group, 8,825 are supporting the internal cybersecurity needs of companies in non-cybersecurity sectors – like manufacturing and healthcare.



4

Louisville is the epicenter of Kentucky's cybersecurity sector.

Louisville is home to about half of the state's cybersecurity companies, as well as associations and conferences focused on the information technology industry. Many of the ingredients needed to create a geographic hub for the cybersecurity sector are already resident in Louisville.

5

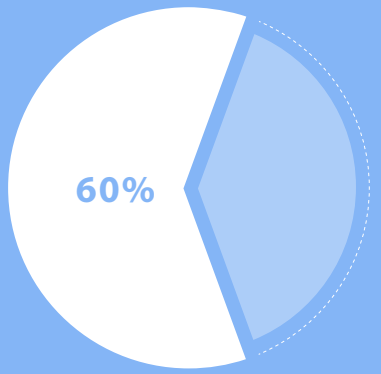
There is a state-level precedent for designing and implementing a tax incentive program to attract cybersecurity companies.

Maryland's Cybersecurity Investment Incentive Tax Credit encourages investments in qualified cybersecurity companies. Two or three companies have participated in the program every year since 2014.

6

Approximately 60% of Kentucky's total cybersecurity workforce is comprised of three job categories.

Computer systems administrators, computer and information systems managers, and computer systems analysts are the most common cybersecurity occupations in the Commonwealth.



7

CYBERSECURITY EARNINGS ARE UP

Cybersecurity workers earn far more than the average Kentuckian.

Workers in every cybersecurity occupation earn more – on average – than Kentucky's annual mean wage of $41,760. Some workers, like computer and information systems managers, earn more than double that figure. Knowledge economy skillsets command higher wages, and the cybersecurity sector in Kentucky is no exception.

CYBERSECURITY DEMAND IS LOW

8

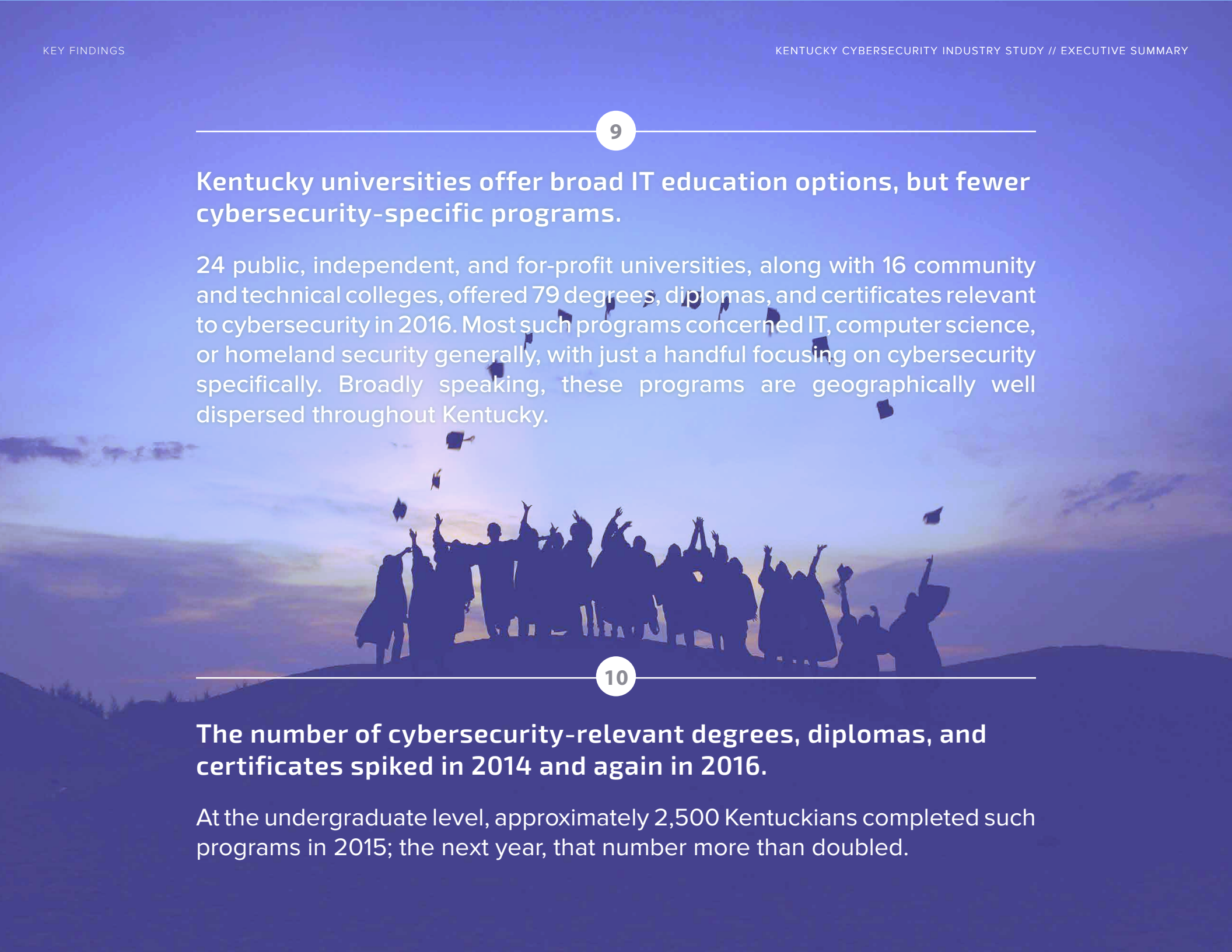
Demand for cybersecurity workers in Kentucky is relatively low.

Kentucky's demand for workers in nearly every cybersecurity occupation is lower than the national average for that occupation, reflecting a greater need (from an economic development perspective) for information technology companies generally and cybersecurity companies specifically.

9

Kentucky universities offer broad IT education options, but fewer cybersecurity-specific programs.

24 public, independent, and for-profit universities, along with 16 community and technical colleges, offered 79 degrees, diplomas, and certificates relevant to cybersecurity in 2016. Most such programs concerned IT, computer science, or homeland security generally, with just a handful focusing on cybersecurity specifically. Broadly speaking, these programs are geographically well dispersed throughout Kentucky.



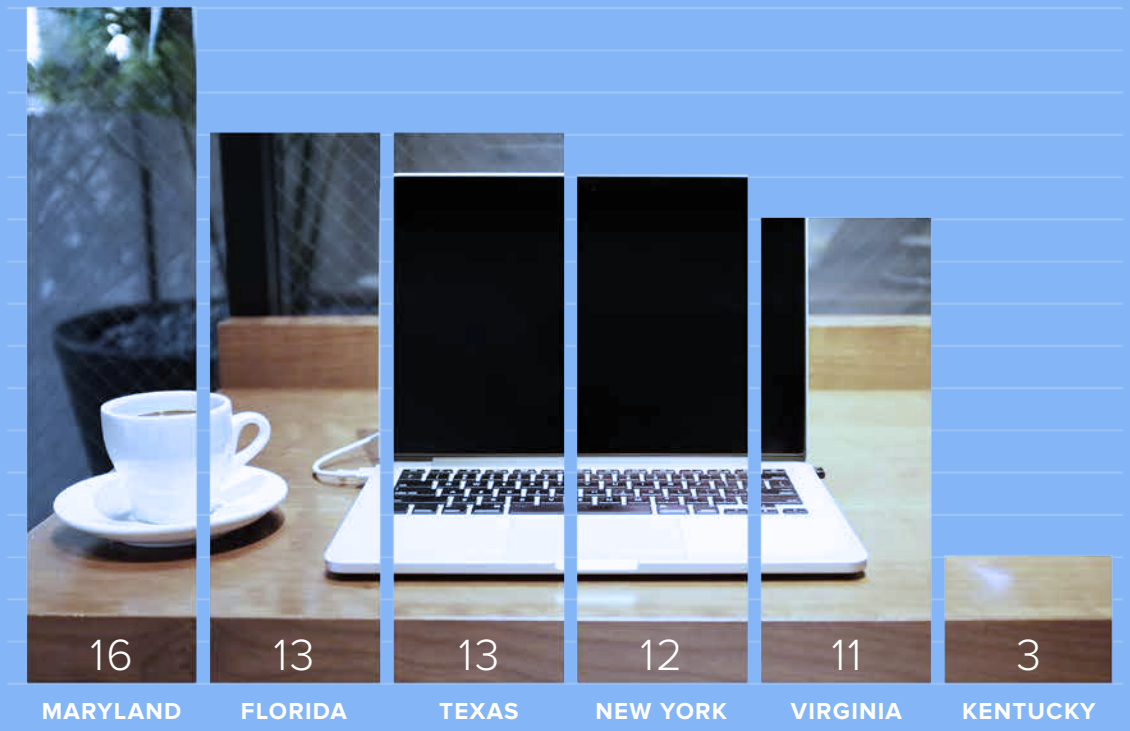
10

The number of cybersecurity-relevant degrees, diplomas, and certificates spiked in 2014 and again in 2016.

At the undergraduate level, approximately 2,500 Kentuckians completed such programs in 2015; the next year, that number more than doubled.

11 Kentucky has three Centers for Academic Excellence in Cyber Defense.

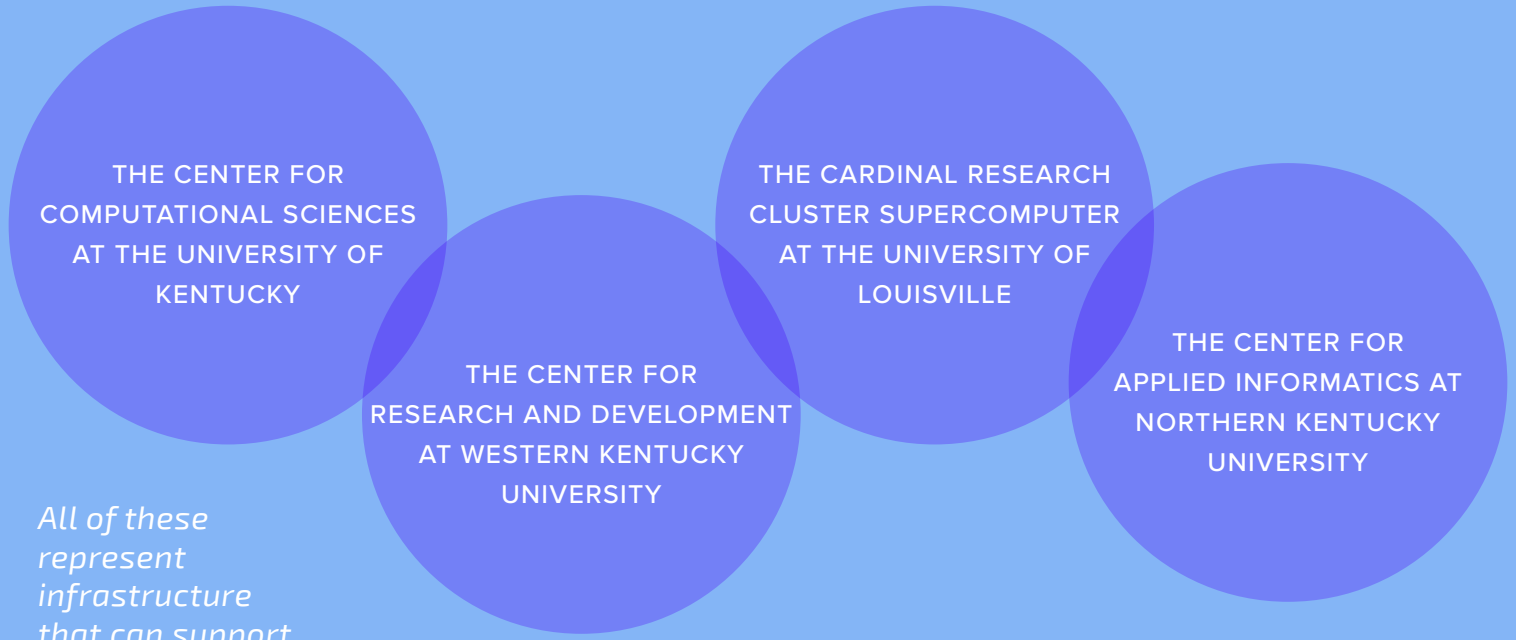
The National Security Agency and the Department of Homeland Security have designated Northern Kentucky University, the University of Louisville, and (most recently) the University of the Cumberlands as Centers for Academic Excellent in Cyber Defense (CAE-CDs).



With only three CAE-CDs, Kentucky trails the country's leading cybersecurity states: Maryland (16), Florida (13), Texas (13), New York (12), and Virginia (11). Kentucky's three CAE institutions are also only for cyber defense education; none are designated for research or for two-year programs.

Other states have a mix of all three CAE-CD programs, which gives them a more balanced impact on the cybersecurity workforce. And although CAEs for Cyber Operations are less common, Kentucky has none.

12 Kentucky has at least four institutions that can enable cybersecurity research and development.



All of these represent infrastructure that can support cybersecurity innovation.

13 There are eight organizations that provide cybersecurity-related training at 13 locations in Kentucky.

Even though training is available online for each of the 19 certifications that we reviewed, there is a lack of brick-and-mortar training locations in the eastern and southeastern parts of Kentucky. CompTIA Security+ and the (ISC)2 Certified Information Systems Security Professional (CISSP) certifications are most often regarded as the most important certifications by respondents to our industry survey.

14

Thousands of people who received a cybersecurity-relevant education in Kentucky are also currently employed in Kentucky.

Of those individuals who were issued a relevant degree, diploma, or certificate in Kentucky in the 11-year period between 2006 and 2016, there were a total of 12,027 individuals employed in Kentucky in the 2015-16 fiscal year.

The technology and education sectors are two of the leading employers of these individuals. However, many work for employers that naturally have low demand for information technology expertise – such as supermarkets, restaurants, and temp agencies.

12,027

INDIVIDUALS EMPLOYED IN KENTUCKY RECEIVED A CYBERSECURITY-RELEVANT EDUCATION IN KENTUCKY

15

Just 18% of Kentucky workers who received a cybersecurity-relevant education in Kentucky are female.

This stark gender gap in the technology industry is not Kentucky's challenge alone, but it is one that should be addressed directly in order to realize the full economic benefits of the cybersecurity economy.

16

Kentucky is taking a leadership role on elementary and secondary cybersecurity education.

Following Louisiana, Kentucky became – in early 2017 – the second state to adopt National Integrated Cyber Education Research Center curricula for elementary and secondary school educators. The Kentucky Department of Education has made the curricula available to all school districts, and Jefferson County Public Schools will be first to put the curricula into effect at the high school level.

17

Kentucky's state government has taken significant steps towards improving its own cybersecurity posture.

Kentucky has established a Chief Information Security Officer; centralized cybersecurity for state agencies through the Commonwealth Office of Technology; created a Financial Cybercrime Task Force; held at least two cybersecurity-focused exercises; recognized cybersecurity in homeland security, law enforcement, and emergency management plans; and formed fundamental homeland security and information sharing partnerships. The Kentucky Intelligence Fusion Center is also ramping up its cybersecurity program.

18

Kentucky has two state laws that address key cybersecurity issues.

House Bill 5 compels the state government to develop a framework for the protection of personally identifiable information (PII) and establishes requirements for what must happen if such information is compromised. House Bill 232 requires non-government holders of PII (like businesses and individuals) to notify any individual whose PII was compromised. However, Kentucky does not require businesses and individuals to notify the state government of such a compromise. As a result, there is no mechanism for the state to track these incidents. Some other states require businesses and individuals to notify the Attorney General.

19

The Kentucky Army National Guard is a national leader in cybersecurity.

Kentucky is home to a nationally competitive National Guard cybersecurity unit. The National Guard has announced plans to establish an Army National Guard Cyber Protection Team in the Commonwealth by FY19. This new unit has the potential to add immense value in defining and maturing cybersecurity assessment, protection, response, and recovery processes.

20

Kentucky lacks a comprehensive public awareness program for cybersecurity.

COT and the Office of Attorney General host cybersecurity resource pages on their websites, which provide a starting point for the state's public awareness effort. However, the state lacks a comprehensive program for businesses (to help them establish baseline capabilities, user awareness, and risk management processes) and residents (to improve cybersecurity habits and awareness).

21

Six states have established Chief Privacy Officer (CPO) positions.

While CPOs typically serve as the state government's lead resource on privacy issues, some also have a public-facing function designed to increase citizen awareness of privacy considerations. CPO roles also include best practice promotion, policy recommendation, training and education, technology regulation advice, and stakeholder engagement.

22

More than 20 states have established a multi-stakeholder cybersecurity initiative.

Variable factors include structure, purpose, type, authority, method of establishment, and number and responsibilities of participants. While some states focus primarily on improving the state government's cybersecurity posture, other initiatives address education, workforce, economic development, information sharing, and a host of issues that concern the private sector and individual residents, as well.

RECOMMENDATIONS

Kentucky already has many of the key ingredients it needs to realize the economic and security benefits of a vibrant cybersecurity sector. With purposeful action tied to strategic direction, it can put those ingredients to work.

Kentucky can become a recognized hub for cybersecurity companies and talent, and it can be a national leader in protecting citizens, businesses, and infrastructure from cyber risk.

Guided by our findings, our report makes dozens of specific, actionable, and practical recommendations. Here, we highlight the 22 most salient recommendations identified in the study.

KENTUCKY CYBERSECURITY COUNCIL

CO-CHAIRS

GOVERNOR OR LIEUTENANT GOVERNOR

INDUSTRY EXECUTIVE

PERMANENT STAFF

EXECUTIVE DIRECTOR

DEPUTY DIRECTOR

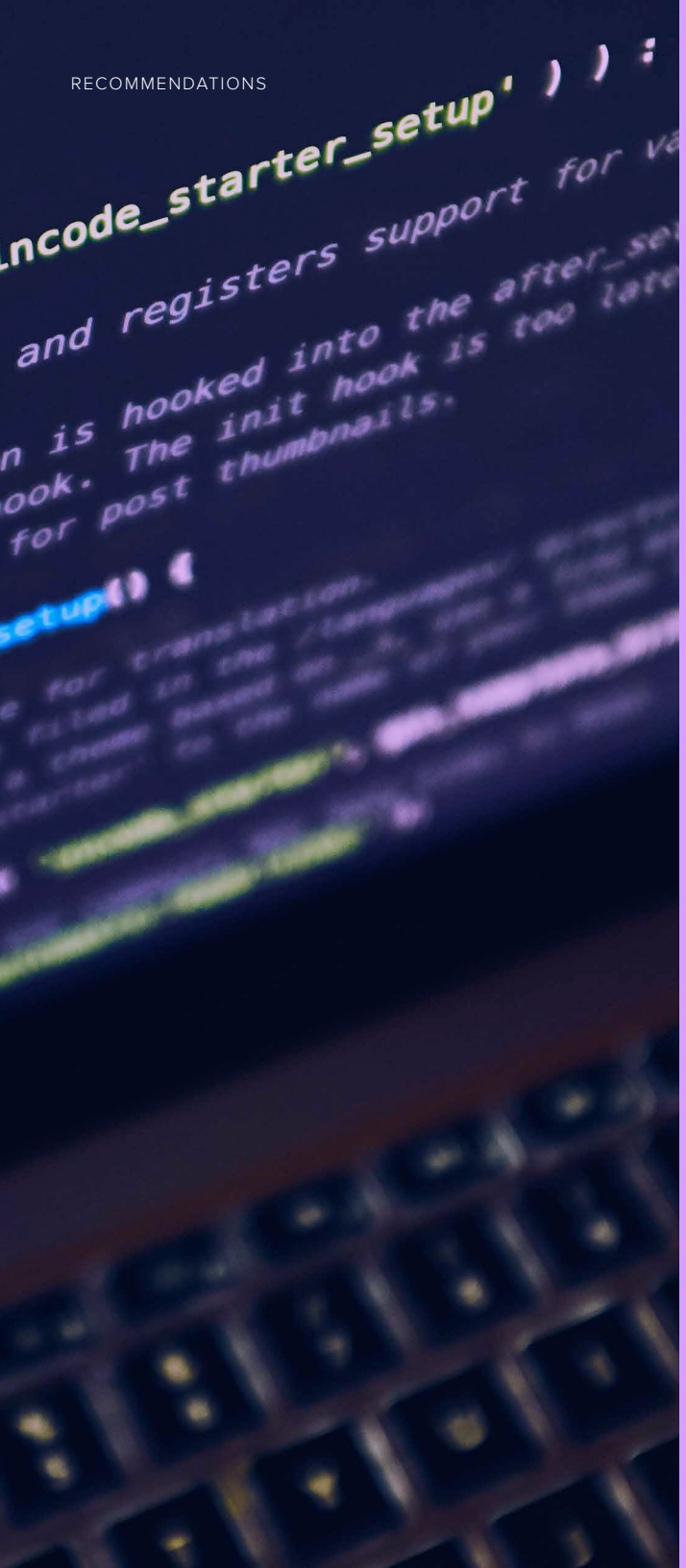
EXECUTIVE ASSISTANT

COMMITTEES

TITLE	LEAD AGENCY
ECONOMY & INNOVATION	CABINET FOR ECONOMIC DEVELOPMENT
WORKFORCE & EDUCATION	COUNCIL ON POSTSECONDARY EDUCATION
CRITICAL INFRASTRUCTURE	KENTUCKY OFFICE OF HOMELAND SECURITY
MILITARY & VETERANS AFFAIRS	KENTUCKY COMMISSION ON MILITARY AFFAIRS
PUBLIC AWARENESS	KENTUCKY OFFICE OF HOMELAND SECURITY
PRIVACY	COMMONWEALTH OFFICE OF TECHNOLOGY

1 Establish the Kentucky Cybersecurity Council (KCC).

Kentucky should establish a comprehensive cybersecurity initiative that serves as the vehicle for implementing most of the recommendations in this report. The KCC should be forward-leaning, action-oriented, and collaborative. The KCC should be a permanent organizational unit attached to the Office of the Governor, and it should be co-chaired by the Governor or Lieutenant Governor and an industry executive. It should have three permanent government staff members and six committees comprised of both public and private sector members. The committees should cover: economy and innovation; workforce and education; critical infrastructure; military and veterans affairs; public awareness; and privacy. If the state government opts to create a Chief Privacy Officer position within the Commonwealth Office of Technology, that individual should lead the privacy committee.



2 Develop a statewide cybersecurity strategy.

The Kentucky Cybersecurity Council should build on the findings of this study to develop a comprehensive statewide cybersecurity strategy. The strategy should be sweeping in scope but practical in design, and it should have achievable goals tied to measurable objectives that yield clearly defined outcomes.

3 Develop and promote a cybersecurity brand for Kentucky.

Kentucky will need to brand and promote its cybersecurity niche in order to appeal to the workers and companies that will build the cybersecurity economy. Focus on Kentucky's assets – both in terms of industry and in terms of lifestyle – and contextualize them for innovators and investors. We recommend a comprehensive communications effort that includes strategic planning, stakeholder engagement, and marketing.

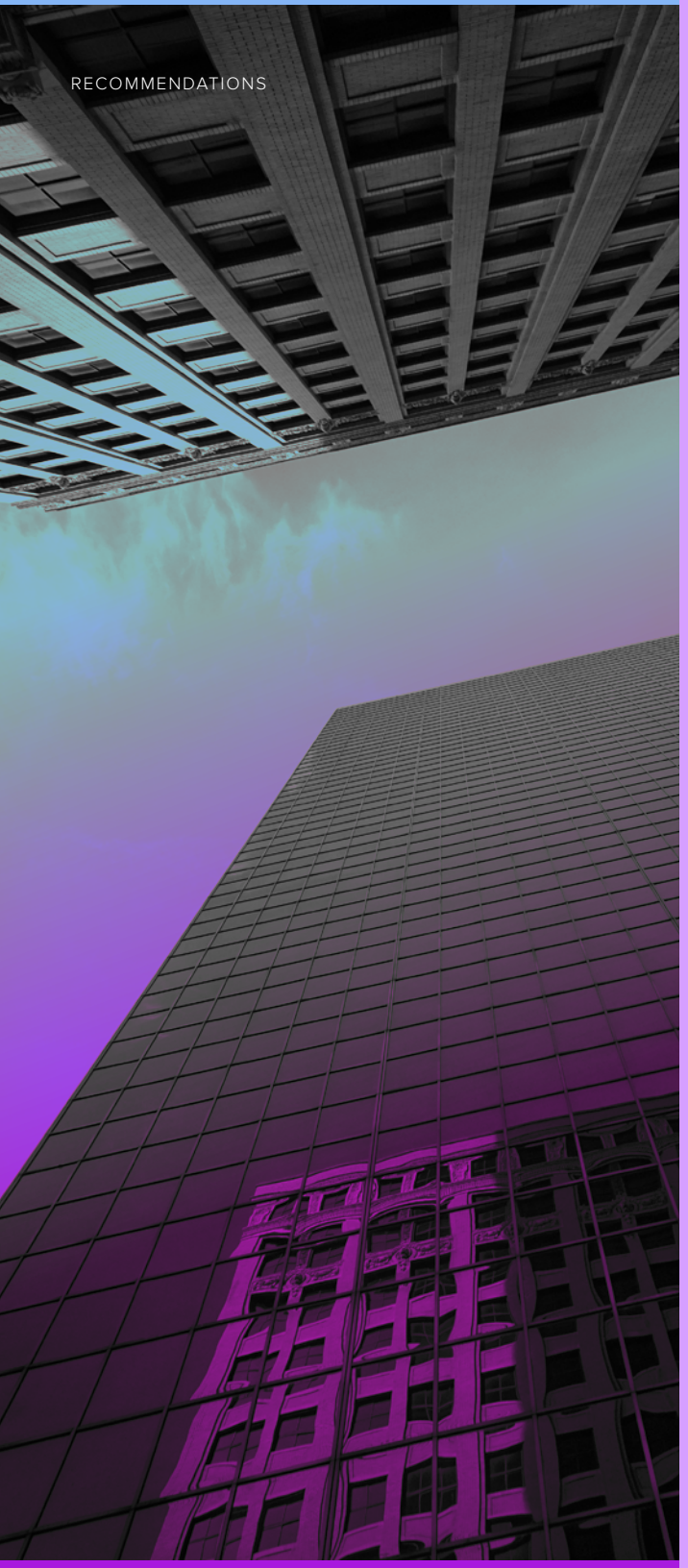
4 Launch a public awareness campaign.

The cybersecurity planning guidelines we outline in this report should be validated, consolidated, and promoted in order to encourage business and citizen awareness of cybersecurity best practices. The campaign would include several discrete components, including (but not limited to):

- ***Cybersecurity resource website.*** A "one-stop shop" for businesses and citizens to access cybersecurity resources, learn about the latest risks and best practices, and to report incidents on their networks. While not endorsing a specific methodology or product, the website should include available government resources, non-commercial assessment tools, standards, information sharing organizations, and community best practices. The website should also have a specific section dedicated to privacy resources, to include tips, best practices, and white papers.

- ***Cybersecurity and privacy guidebooks.*** Clear, simple, and visually appealing guides to cybersecurity and privacy fundamentals for businesses and citizens, endorsed by the KCC.

- ***Marketing.*** Even though it's a public policy issue, cybersecurity should be the subject of a marketing campaign not unlike ones brands use to promote their products.



5 Establish a cybersecurity hub.

Investors and innovators need a dot on the map. They are drawn to thriving hubs of activity that are already attracting other investors and innovators. Louisville has organically become the center of Kentucky's information technology industry. With a strong foundation of technology associations, conferences, and academic institutions, Louisville is well positioned to be the focus of attention. State and local leaders should work collaboratively on initiatives to bolster cybersecurity on the city's economic agenda.

6 Invest in research and development.

With excellent R&D infrastructure at universities throughout the Commonwealth, state government leaders should encourage investments in discrete cybersecurity initiatives. Specific attention should be given to commercializing technologies so that the results of R&D efforts can be brought to market by Kentucky companies. Another avenue for R&D investment could be a statewide competition for innovative cybersecurity research. The idea creates additional opportunities – like corporate sponsorship, incentivizing companies to establish a location in Kentucky, and so on.

7 Establish targeted economic incentives to cultivate the cybersecurity sector.

Kentucky needs to create and attract cybersecurity companies – particularly the cutting-edge businesses that will create "buzz" for the Commonwealth. An economic incentive program designed to specifically attract a small but critical mass of such companies will provide the momentum needed to attract others to the state. If Kentucky chooses to become one of the first states in the nation to develop such a program, Maryland's Cybersecurity Investment Incentive Tax Credit should be used as a frame of reference. The Kentucky Enterprise Fund and the Kentucky Business Investment Program represent existing frameworks that can be readily repurposed for attracting cybersecurity companies. The Commonwealth should ensure that additional focus be given to entrepreneurs who are looking for a place to launch their business.

8 Help existing companies pivot to the cybersecurity sector.

For certain companies in adjacent industries (like defense), the cybersecurity sector represents an opportunity to grow their businesses and diversify their revenue streams. Kentucky should consider making business consulting services (like strategic planning and communications) available to qualified companies that want to pursue growth opportunities in the cybersecurity industry.

9 Invest in incentives for Kentucky-based organizations to improve their cybersecurity.

Consider hosting a conference on cyber insurance; funding risk assessments for critical infrastructure assets; piloting new technologies for critical infrastructure protection; and investing in processes to help critical infrastructure operators mitigate cyber risk.

10 Host cybersecurity planning workshops.

We recommend making training, technical assistance, and guidance available to businesses. If businesses better understand the cybersecurity challenges that they face and the potential costs associated with cyber risks, they will be more inclined to make the necessary investments in cybersecurity expertise. Workshops could be held monthly or bimonthly in different regions of the Commonwealth. They would be designed to help businesses develop cybersecurity plans by drawing on the guidelines we provide for capability adoption, user awareness, and risk management.

11 Increase cybersecurity education opportunities at the university level.

A diversified and sophisticated cybersecurity education system is vital to a competitive cybersecurity workforce. The Commonwealth must take concrete steps, such as establishing university scholarships and expanding cybersecurity programs at universities. Particular attention should be paid to increasing access to cybersecurity education among females (to address the stark gender gap), residents of eastern Kentucky (where cybersecurity education opportunities lag behind other parts of the state), and other underrepresented groups.

12 Bring cybersecurity education to elementary and middle schools.

While the adoption of the Cyber Engineering Pathway Curricula is an excellent first step, its near-term rollout is limited to the high school level. Cybersecurity education should begin earlier; children interact with technology every day, and the concepts of proper cyber hygiene should be taught at an early age. While the primary purpose would be to cultivate a cyber-savvy population, this effort would have the ancillary benefit of widening the funnel for the future cybersecurity workforce.

13 Establish the Commonwealth Cybersecurity Committee (C3).

Building on existing cybersecurity efforts within the Commonwealth Office of Technology and across state government, Kentucky should establish the C3. Led by Kentucky's Chief Information Security Officer, the C3 would conduct risk assessments for state government assets; oversee compliance with technical control programs; and oversee a training program for all government employees, among other functions.

14 Formalize a concept of operations for the cybersecurity mission of the Kentucky Intelligence Fusion Center (KIFC).

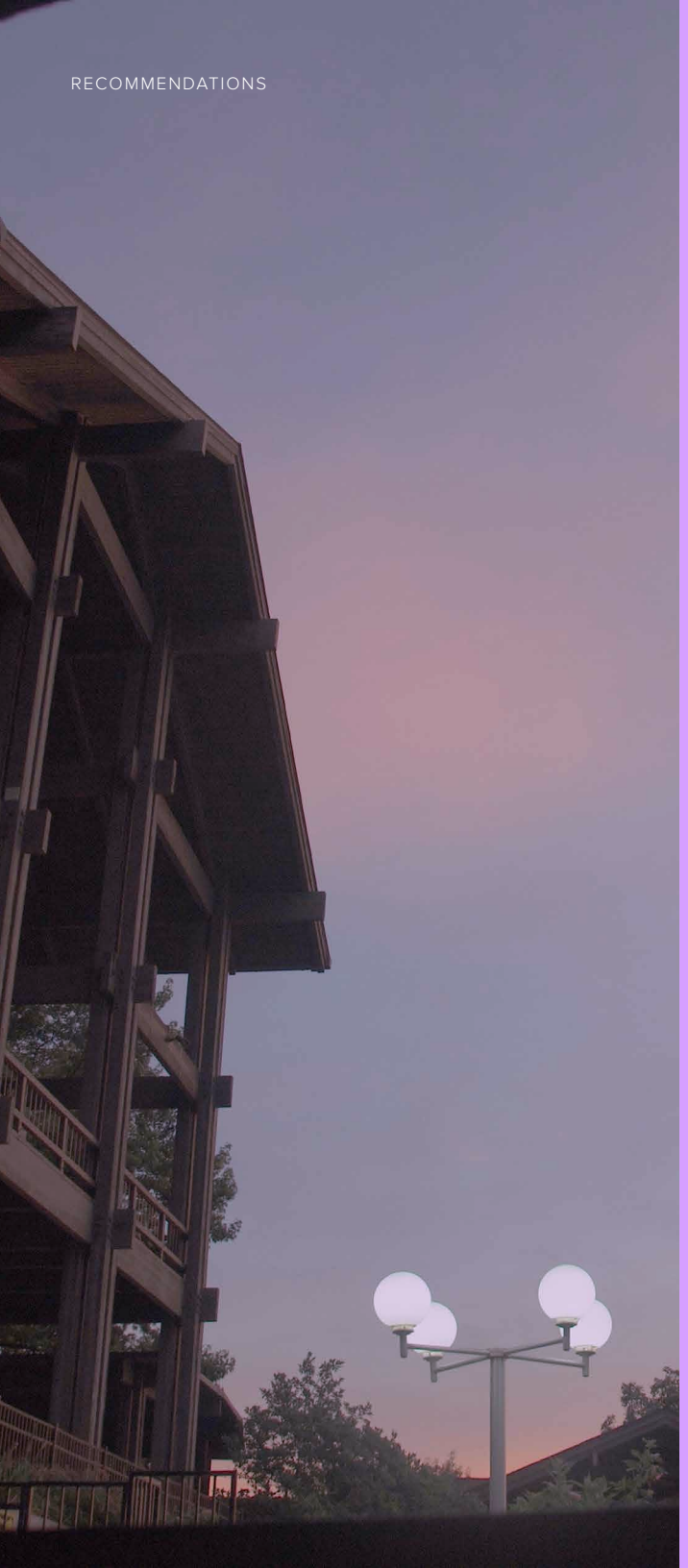
The KIFC is well positioned to be the “one-stop shop” for the sharing of cybersecurity information between government and industry. This expansion of KIFC’s role should be met with sufficient resourcing to ensure it can fulfill this vital function.

15 Adopt the proposed Kentucky Cyber Critical Infrastructure (CCI) Risk Management Process.

Following a validation process by KIFC and key stakeholders, we recommend that the process become KIFC’s approach to identifying and managing risk across the Commonwealth’s CCI. For the first iteration of this process, KIFC should host a full-day workshop for key stakeholders from KOHS and Kentucky’s sector-specific agencies. The purpose will be to educate stakeholders on the CCI Risk Management process and to generate a comprehensive list of assets in question (AIQs). Stakeholders should nominate AIQs on an annual basis, although a refresher workshop may be necessary on a biennial basis.

16 Designate state-level sector-specific agencies.

While the responsibility for coordinating critical infrastructure protection efforts in Kentucky falls to KOHS, we recommend that Kentucky mirror the Federal framework of assigning a sector-specific agency for each of the 16 critical infrastructure sectors.



17 Expand the data breach notification law.

When a business or individual experiences a security breach that results in the loss of PII, they are required to notify the citizens whose PII was affected, but not the government. The Kentucky legislature should require those individuals and businesses to also notify the Office of Attorney General of the breach and PII loss.

18 Integrate cybersecurity into the Emergency Operations Plan.

The EOP does address the threat of cyber terrorism, and it has a well-documented concept of operations for Emergency Support Function (ESF) 2: Communications. Moreover, COT has a cyber incident response plan for state government functions. However, the EOP should document the Commonwealth's processes for managing a cyber disruption event that affects cyber critical infrastructure outside of the public sector.

19 Capitalize on the cybersecurity capability of the KYARNG.

The KYARNG is rapidly establishing itself as a cybersecurity leader among its peers in other states. Currently a primary agency for ESF 2, the J6 is already one of the state's foremost cybersecurity centers of excellence. The Commonwealth should consider expanding its cybersecurity roles and authorities in the case of an emergency, provided it is allocated appropriate resources and staff to fulfill additional obligations. As an example, the cyber annex to Washington State's Emergency Management Plan specifically highlights the Governor's authority to activate the National Guard.

20 Formalize Kentucky's cybersecurity exercise program.

The cybersecurity exercises conducted in Kentucky are an excellent starting point for a formal exercise program under the leadership of KOHS. Exercises can be held two or three times per year, with one strategic-level exercise and one or two with an operational focus. To ensure that progress is made in the intervals, each exercise should build on the findings of the previous one, and they should all be deliberately designed to identify gaps in plans and capabilities. Exercises provide an excellent opportunity to understand and strengthen partnerships, so it is critical that Kentucky's military installations are included. Exercise management should include the Homeland Security Exercise and Evaluation Program (HSEEP) phases of foundation, design and development, conduct, evaluation, and improvement planning, as well as necessary coordination and after-action reporting.

21 Organize a government and military CISO roundtable.

Because they are funded by taxpayer dollars and serve the public interest, government and military agencies at the federal, state, and local levels share common concerns and constraints. We suggest that an informal roundtable of major government and military chief information security officers (CISOs) in Kentucky meet on a quarterly basis to discuss best practices and lessons learned. Although their authorities and scopes of responsibility vary significantly, CISOs from COT, the Kentucky National Guard, the Fort Knox NEC, the RNEC-Bluegrass, and major local jurisdictions (like Louisville and Lexington) could work together to address challenges shared by the enterprises they oversee.

22 Conduct another cybersecurity industry study in two years.

We recommend conducting portions of this study (especially economic impact, education, and workforce) again in 2019. This "update" will allow policymakers to assess the progress of the cybersecurity economy over the previous two-year period and allow them to make adjustments as necessary.

ACKNOWLEDGMENTS

In order to better understand Kentucky's cybersecurity industry, we relied on the inputs of many stakeholders, without whom this report would not have been possible. We must give special recognition to the Office of Economic Adjustment and the Kentucky Commission on Military Affairs for their sponsorship of this study; to the Cabinet for Economic Development, which provided economic and labor data courtesy of JobsEQ®, a product of Chmura Economics and Analytics; and the Kentucky Center for Workforce and Education Statistics, which provided workforce and education data. This section does not name the more than 20 people who responded on behalf of their organizations to our industry survey, but we are equally grateful to them for their time and expertise.

OFFICE OF THE LIEUTENANT GOVERNOR OF KENTUCKY

Lieutenant Governor Jenean Hampton

Steve Knipper

KENTUCKY COMMISSION ON MILITARY AFFAIRS

MG (Ret.) Robert Silverthorn

COL (Ret.) Blaine Hedges

1st Lt (Ret.) Stewart Ditto

Stacey Shane

COMMONWEALTH OFFICE OF TECHNOLOGY

David Carter

KENTUCKY NATIONAL GUARD

LTC William Ewing

Dean Kendrick

CPT Dayna Sanders

Jimmy Caudle

DEPARTMENT OF HOMELAND SECURITY

Gregory Howard

Klint Walker

KENTUCKY OFFICE OF HOMELAND SECURITY

John Holiday

Jason Childers

Kayla Matola

KENTUCKY OFFICE OF THE ATTORNEY GENERAL

John Moberly

KENTUCKY EMERGENCY MANAGEMENT

Michael Dossett

COL Wayne Burd

Harry James

Steven Brukwicki

Sharon Goode

CABINET FOR ECONOMIC DEVELOPMENT

Joe Lilly

Caroline Baesler

Karen Lefler

Emmanuel Kyeremeh

Josh Benton

KENTUCKY CENTER FOR EDUCATION AND WORKFORCE STATISTICS

Dr. Kate Akers

Dr. Jessica Cunningham

Barrett Ross

KENTUCKY STATE POLICE

Maj. Jeff Medley

Cpt. Michael T. Kidd

Lt. Jeremy Murrell

Jerry Wright

Angela Parker

TECHNOLOGY ASSOCIATION OF LOUISVILLE KENTUCKY

Dawn Yankeelov

KENTUCKY ASSOCIATION OF MANUFACTURERS

Karen Ellis

VIRGINIA OFFICE OF THE SECRETARY OF TECHNOLOGY

Secretary Karen Jackson

MICHIGAN DEPARTMENT OF MANAGEMENT, TECHNOLOGY, AND BUDGET

David Behen

Rajiv Das

Ashley Gelisse

Caleb Buhs

WASHINGTON OFFICE OF PRIVACY AND DATA PROTECTION

Alex Alben

SOUTH CAROLINA ENTERPRISE PRIVACY OFFICE

Theodora Wills

Alex White

Michele Perrick

WEST VIRGINIA HEALTH CARE AUTHORITY

Sallie Milam

MARYLAND FINANCE PROGRAMS

Mark Vulcan

simon
everett
an analytic design firm

For more information about this study, please contact:

Simon Everett // inquiries@simon-everett.com
Kentucky Commission on Military Affairs // 502.564.2611, extension 302