Hawai‘i Statewide Cyber Workforce Development Strategy

Hawai‘i Office of Homeland Security

January 2025

This page intentionally blank

Table of Contents

This page intentionally blank

Executive Summary

A resilient cyber workforce is crucial in today's digital era, ensuring the protection of sensitive information, mitigating evolving cyber threats, and maintaining continuity of essential services. This workforce is essential for safeguarding our Nation’s critical infrastructure, supporting economic stability, building public trust, advancing technological development, and enhancing national security.

Cybersecurity professionals are needed to protect personal, financial, and strategic data across organizations throughout the State of Hawai‘i. They play a vital role in identifying, preventing, and responding to cyber threats. Their expertise is crucial for rapid recovery from cyber incidents and ensuring uninterrupted business activities and public services. Skilled cybersecurity teams help state organizations continue providing critical services. In our critical infrastructure sectors, a skilled cyber workforce safeguards vital services, preventing severe consequences for public safety and national security. Furthermore, cybersecurity underpins the modern economy by protecting intellectual property, financial transactions, and digital assets, fostering a secure environment for innovation and growth.

As the State’s first comprehensive cyber workforce development strategy, this plan is essential to fortify our digital defenses, protect sensitive information, and ensure operational resilience. This strategy emphasizes the recruitment, development, and retention of skilled cybersecurity professionals who can effectively protect against ever-evolving cyber threats and respond swiftly when incidents do occur. By investing in continuous training and education, we aim to keep our workforce adept at the latest technologies and threat landscapes. The strategy also focuses on fostering a culture of security awareness across the state. By supporting economic stability and technological innovation, our robust cyber workforce will build public trust and enhance our overall security posture, ensuring we are well-prepared to meet the challenges of the digital age and protect our security interests.

Problem

Growing Cyber Workforce Gap: The State of Hawai‘i is faced with a growing shortage of skilled cybersecurity professionals, a critical workforce gap mirrored at the national level. The growing cyber workforce gap poses a significant threat to national security, critical infrastructure, and businesses as the demand for skilled professionals far exceeds the available supply. This shortage leaves organizations vulnerable to cyberattacks and data breaches, undermining their ability to effectively protect access to critical services. Addressing this gap requires immediate investment in cybersecurity education and training to develop a pipeline of qualified experts.

Solution

Statewide Cyber Workforce Development Strategy: The State of Hawai‘i is investing in a whole community, collaborative approach to addressing the cyber workforce gap. The *Statewide Cyber Workforce Development Strategy* is multifaceted, aiming to build and sustain a capable and resilient cyber workforce that can effectively protect Hawai‘i’s digital assets, information systems, and critical infrastructure from cyber-attacks. It provides strategic- and tactical-level recommendations for growing the State’s cyber talent pool and fostering collaboration among government and the private sector.

Strategy

Six-Step Approach: The *Statewide Cyber Workforce Development Strategy* is organized in a six-step approach to achieving the goals and objectives of this strategy. These six steps are interconnected, with each building off and supporting other steps. This interconnected approach builds a cohesive and adaptive strategy that can effectively develop and sustain a robust cyber workforce in Hawai‘i. These six strategic areas include: Education and Training, Recruitment and Retention, Continuous Learning and Development, Partnerships and Collaboration, Adaptability and Flexibility, and Diversity and Inclusion.

Implementation

Implementation Plan: The *Statewide Cyber Workforce Development Strategy* includes an implementation plan consisting of 30 activities aimed at creating an actionable path forward for achieving the goals and objectives defined in the statewide strategy. These activities are organized under the six strategic areas of the strategy, creating a roadmap for building and sustaining the State’s cyber workforce. The State and Local Cybersecurity Grant Program Chartered Working Group, via the Hawai‘i Office of Homeland Security, are charged with management of the Implementation Plan.

Frank J. Pace
Administrator
Hawaii Office of Homeland Security
January 17, 2025

Introduction

The Hawai‘i *Statewide Cyber Workforce Development Strategy* is critical for addressing the pervasive and growing shortage of skilled professionals in the cybersecurity field. The cyber landscape is becoming increasingly complex, with cyber threats evolving in sophistication and frequency. Despite this, the supply of qualified cybersecurity professionals is not keeping pace with demand. The *ICS2 2023 Cyber Workforce Study* states that as of 2023, the U.S. faces a shortfall of approximately 522,000 cybersecurity professionals, a gap that is projected to widen as digital transformation accelerates.[1]

"… [W]e are in the midst of a fundamental transformation in our Nation's cybersecurity. It is now clear that a reactive posture cannot keep pace with fast-evolving cyber threats and a dynamic technology landscape, and that aspiring just to manage the worst effects of cyber incidents is no longer sufficient to ensure our national security, economic prosperity, and democratic values." - *2024 Report On The Cybersecurity Posture of The United States*[2]

This shortage poses significant risks to national security, organizational stability, and economic growth in Hawai‘i. Without a well-trained, resilient cyber workforce, public and private organizations in Hawai‘i are vulnerable to data breaches, financial loss, and operational disruptions. A strategic approach to developing this workforce is essential to mitigate these risks and to ensure that both public and private sectors can protect their assets and information from malicious actors and cyber disruptions. This strategy underscores the urgency and importance the State of Hawai‘i has placed on promoting a strong, resilient cyber workforce.

Purpose

The purpose of the *Statewide Cyber Workforce Development Strategy* is multifaceted, aiming to build and sustain a capable and resilient cyber workforce that can effectively protect Hawai‘i's digital assets, information systems, and critical infrastructure from cyber-attacks.

[1] ICS2 2023 Cyber Workforce Study, https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf?rev=28b46de71ce24e6ab7705f6e3da8637e

[2] 2024-Report-on-the-Cybersecurity-Posture-of-the-United-States.pdf (whitehouse.gov)

Goals and Objectives

The following goals and objectives of the *Statewide Cyber Workforce Development Strategy* have been identified to ensure Hawai‘i has the necessary talent and skills to protect against the cyber threats of today and of the future.

Goals

1. Develop and enhance the technical skills of cybersecurity professionals through training programs, workshops, and certifications to keep the workforce updated with the latest technologies, tools, and best practices in cybersecurity.
2. Foster the recruitment and retention of cybersecurity talent through initiatives such as marketing, outreach programs, internships, and career development opportunities.
3. Create the conditions to build a resilient cybersecurity workforce through identifying training and development opportunities, to include non-technical soft skills, so that organizations can build a workforce capable of effectively responding to an ever-evolving cyber threat landscape.
4. Promote entrepreneurial conditions and foster innovation to attract cybersecurity business to Hawai‘i.

Objectives

1. Provide a mechanism to effectively coordinate among existing workforce, to include both cybersecurity-focused and general workforce development efforts.
2. Consolidate and promote existing cybersecurity professional development opportunities in Hawai‘i.
3. Establish marketing campaign for recruiting cybersecurity talent across multiple demographics.
4. Establish outreach programs targeting K-12 students to promote awareness and interest in the cybersecurity profession.
5. Create a mechanism for conducting annual reviews of the current cybersecurity workforce in Hawai‘i to identify gaps in workforce or skills.
6. Develop performance metrics to monitor progress towards the goals and objectives of the *Statewide Cyber Workforce Development Strategy*.

Assumptions

In preparing the *Statewide Cyber Workforce Development Strategy*, several key assumptions were made to guide the analysis, conclusions, and recommended courses of action. These assumptions are based on available researched data, standard industry practices, and relevant historical trends. They serve as the foundation for the method and interpretation of the contents presented in this strategy. Those assumptions include:

1. The strategy aligns with roles, responsibilities, and authorities outlined in Hawaii Revised Statutes §128B Cybersecurity;
2. In the spirit of Hawaii Revised Statutes §128B Cybersecurity, other departments, agencies, and private companies, both inside and outside of the State will be make a best effort to support the Office of Homeland Security (OHS) in carrying out its relevant roles and responsibilities;
3. Operationalization of this strategy is the responsibility of OHS, in coordination with the State and Local Cybersecurity Grant Program (SLCGP) Chartered Working Group (CWG);
4. OHS may delegate implementation activities to other entities but retains overall responsibility for meeting the goals and objectives outlined in the strategy;
5. Milestones and timelines will be defined and tracked following approval of the strategy;
6. If portions of the NICE framework are found to be inapplicable to the State or any department or agency, the applicable portions will still apply;
7. The K-12 strategy is consistent with the strategy the Hawai‘i Department of Education (DOE) is currently following; and
8. The State does not consider non-residents as part of its workforce.

Dependencies

This section outlines the critical dependencies that influence the outcomes and implementation of the strategy’s recommendations. These dependencies include external factors, resources, and systems that must be in place for the proposed strategies to succeed. Understanding these dependencies is essential for assessing the feasibility and risks associated with the strategy.

1. A budget is authorized and available for State departments and agencies to hire and/or retrain staff to support implementation of this strategy;
2. State departments and agencies will make necessary adjustments to support this strategy and its implementation;

3. State Departments of Personnel Management, or similar groups, must agree to allow cybersecurity requirements specified under this strategy to be included in all state job descriptions (as applicable) and to include them in performance reviews;
4. Management in all State department and agencies management must actively adopt cybersecurity leadership principles; and
5. The pool of in-state and out-of-state qualified workers is sufficient to fill positions critical to the success of this strategy.

Governance

Effective cybersecurity leadership within the State is essential for the success of this strategy. As cybersecurity is recognized as a shared responsibility, establishing a separate, dedicated layer of security-focused leadership alone will not ensure the implementation of cybersecurity principles across all State departments and agencies. Instead, these principles must be incorporated into the roles of all managers and supervisors to embed them into the organization's culture. Security leadership practices, such as those recommended by the Cyber Readiness Institute[3], should be adopted at both the individual and departmental levels to foster a comprehensive and resilient cybersecurity framework.

The State of Hawai'i, as a recipient of the SLCGP grant, has established an SLCGP CWG. The SLCGP CWG administers and oversees all activities using these grant funds. As such, the SLCGP CWG will play a key role in the governance and implementation of the *Statewide Cyber Workforce Development Strategy*.

To support the development of the Hawai'i *Statewide Cyber Workforce Development Strategy*, the SLCGP CWG and the Hawai'i OHS organized an interagency working group including 88 individuals representing 39 different federal, state, county, non-profit, and private sector organizations. The working group member organizations include the following (listed alphabetically):

- City and County of Honolulu
- ClimbHI
- County of Hawai'i
- County of Kaua'i
- County of Maui
- Cyber Hui
- Cyber Hawai'i

[3] https://cyberreadinessinstitute.org/

- Department of Accounting and General Services
- Department of Attorney General
- Department of Business, Economic Development, & Tourism
- Department of Education
- Department of Health
- Department of Homeland Security
- Department of Human Services
- Department of Labor
- Department of Transportation
- DRFortress
- Hawai‘i Gas
- Hawai‘i Health Systems Corp.
- Hawai‘i National Guard
- Hawai‘i Pacific University
- Hawai‘i Technology Development Corporation
- Hawai‘i an Electric Company
- Honolulu Community College
- Infraguard Hawai‘i
- Kauai Department of Water
- Kauai Island Utility Cooperative
- Leeward Community College
- Legislature, House
- Legislature, Senate
- Office of Hawai‘i an Affairs
- Office of Homeland Security
- Office of the Governor
- Par Pacific
- State Energy Office
- Teamworx
- The Queen's Health System
- U.S. Army National Guard
- U.S. Cybersecurity and Infrastructure Security Agency
- University of Hawai‘i

Current State of the Workforce

The current state of the cybersecurity workforce in the United States is marked by a significant shortage of professionals. The U.S. faces a cybersecurity workforce gap of approximately 522,000 professionals, reflecting a 19.7% increase from the previous year. The ICS2 2023 Cyber Workforce Study noted that nearly all organizations have cybersecurity skills gaps with 92% of surveyed cybersecurity professionals saying their organization suffers from skills gaps in one or more areas (see Figure 1 below).[4] This shortage is part of a broader global trend, where the demand for cybersecurity professionals consistently exceeds supply. Workforce shortages of cybersecurity professionals result in more than a personnel challenge. This workforce gap directly impacts organizations' ability to prevent and mitigate the effects of cyber-attacks. This broader, nationwide workforce gap is mirrored in Hawai'i, resulting in a direct impact on the State's ability to mitigate, respond to, and recover from cyber incidents.

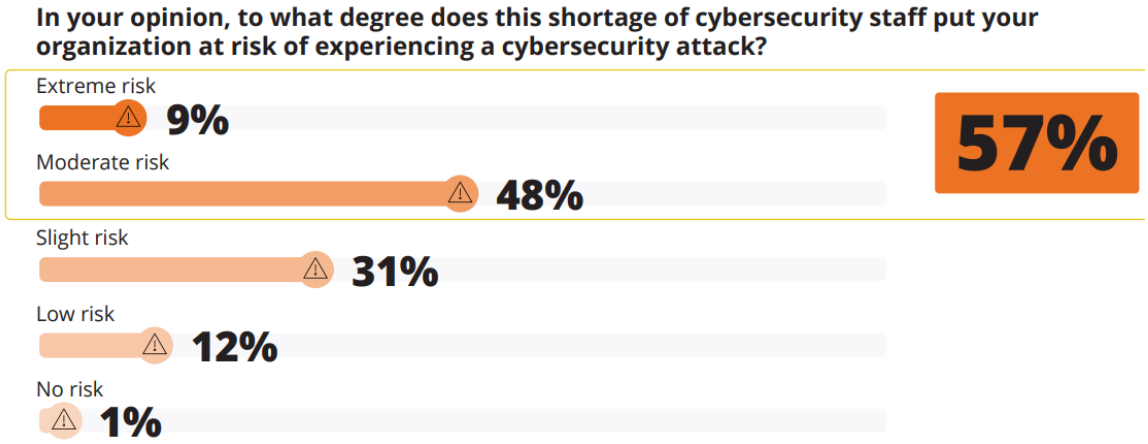


Figure 1: ICS2 2023 Cyber Workforce Study

Hawai'i s Cyber Workforce Gap

CyberSeek, a program supported by the National Initiative for Cybersecurity Education (NICE), a program of the National Institute of Standards and Technology in the U.S. Department of Commerce, estimates the total employed cybersecurity workforce in Hawai'i to be 7,196 individuals. The study also estimates there are 4,534 cybersecurity-related job openings in the State. This calculates to a supply-demand ratio of 73%, which CyberSeek defines as the,

[4] ICS2 2023 Cyber Workforce Study, https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf?rev=28b46de71ce24e6ab7705f6e3da8637e

"comparison of the number of available cybersecurity workers relative to employer demand in a particular location, displayed as a percentage."[5]

Transition from Service-Based Economy

Hawai'i, as a small, remote, non-contiguous state, is presented with unique workforce challenges. These challenges are complex and, in part, directly tied to the fundamental structure of Hawai'i's economy. A 2021 report by the Hawai'i Department of Business, Economic Development and Tourism noted that, "[t[he top three industries with the largest employment for the U.S. were Healthcare and Social Assistance (14.0%), Retail Trade (11.2%), and Manufacturing (10.2%), whereas the top three industries in Hawai'i were Accommodation and Food Services (14.4%), Healthcare and Social Assistance (11.6%), and Retail Trade (11.1%)."[6] Hawai'i is predominantly a service-based economy with a relatively small job market and the highest cost of living in the Nation. The long-sought major economic diversification beyond tourism has not occurred. Smaller but important "non-traded clusters" of employers including state and local government, defense, agriculture, construction, and others exist, but hospitality remains dominant, an industry reliant on low-skilled and low-wage service jobs.

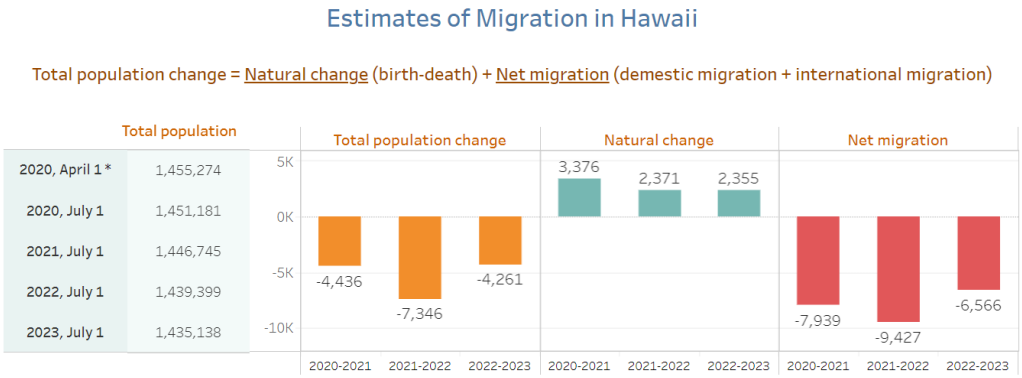
Educational Alignment with Cyber Workforce Gap

It is essential to build and sustain strategies which promote education programs to grow the cyber workforce. The Hawai'i Workforce Funders Collaborative noted in a 2020 report that, "[a] mismatch between educational attainment and labor-market needs is a threat to the state's economic health."[7] The report continues with, "In 2008, state leaders set a goal that 55 percent of working-age adults would hold postsecondary degrees by 2025. However, Hawai'i is not yet on track to achieve that goal. In the ten years after the goal was set, the state's postsecondary attainment rate grew only slightly, from 42 percent to 46 percent. And even if the state reaches its goal, 55 percent falls short of the state's talent needs. Projections showed that, by this year, 70 percent of jobs in the state will require some postsecondary education."[8] This strategy aims to promote educational programs that will support building a sustaining a strong cyber workforce in Hawai'i.

[5] https://www.cyberseek.org/heatmap.html
[6] Hawaii DBEDT, *Hawaii's Working Population: An Analysis by Industry*, https://files.hawaii.gov/dbedt/economic/reports/Hawaii_Workforce_Report_2021.pdf
[7] *A Talent Roadmap to Support Economic Recovery in Hawai'i* , https://static1.squarespace.com/static/640a4ca03eff8f1ba217a185/t/66b3e3012fd6b6377611b3d0/1723065092969/HI-roadmap-Final-090220+%282%29+%281%29.pdf
[8] Ibid

Talent Outmigration

In addition to addressing the existing cyber workforce gap in Hawai‘i, this strategy also aims at providing opportunities to keep native-born Hawai’ians on the islands. A 2021 report from the Hawai‘i Department of Business, Economic Development, and Tourism (DBEDT) noted that, “the population decline in the past three years [has] been primarily attributed to a high rate of net domestic outmigration (see Figure 2 below). Even more so, the popular sentiment is that much of this outmigration is of young, educated workers, a phenomenon sometimes referred to as “brain drain.”[9] Brain drain refers to the emigration of highly skilled or educated individuals from one region to another. This phenomenon typically occurs when professionals, such as scientists, engineers, or IT specialists, leave their home state in search of better career opportunities, higher wages, and/or improved living conditions elsewhere. Brain drain can result in a loss of talent and expertise in the originating location, potentially hindering its economic development and innovation capabilities. It can also lead to a shortage of skilled professionals needed to address local challenges and advance various sectors within the home country or region.[10]



Period	Net migration	Domestic migration	International migration
2020-2021	-7,939	-9,982	2,043
2021-2022	-9,427	-15,664	5,917
2022-2023	-6,566	-11,193	4,627

Source: U.S. Census Bureau, Population Estimates Program, Vintage 2023 State Population Totals and Components of Change: 2020-2023

Figure 2: https://dbedt.hawaii.gov/economic/migration-dashboard/

[9] Hawaii DBEDT, *Brain Drain: Characteristics of Hawai‘i-Born Adults on the U.S. Mainland*, https://files.hawaii.gov/dbedt/economic/reports/Brain_Drain_Hawaii_Born_Population.pdf

[10] U.S. Joint Economic Committee, *Brain Drain across the United States*, https://www.jec.senate.gov/public/index.cfm/republicans/2019/4/losing-our-minds-brain-drain-across-the-united-states

Six-Step Approach

This *Statewide Cyber Workforce Development Strategy* includes a six-step approach to achieving the goals and objectives of this strategy. These six steps are interconnected, with each building off and supporting other steps. This interconnected approach builds a cohesive and adaptive strategy that can effectively develop and sustain a robust cyber workforce in Hawai‘i. Each of these steps is detailed in subsequent sections, along with actionable activities to implement each strategy.

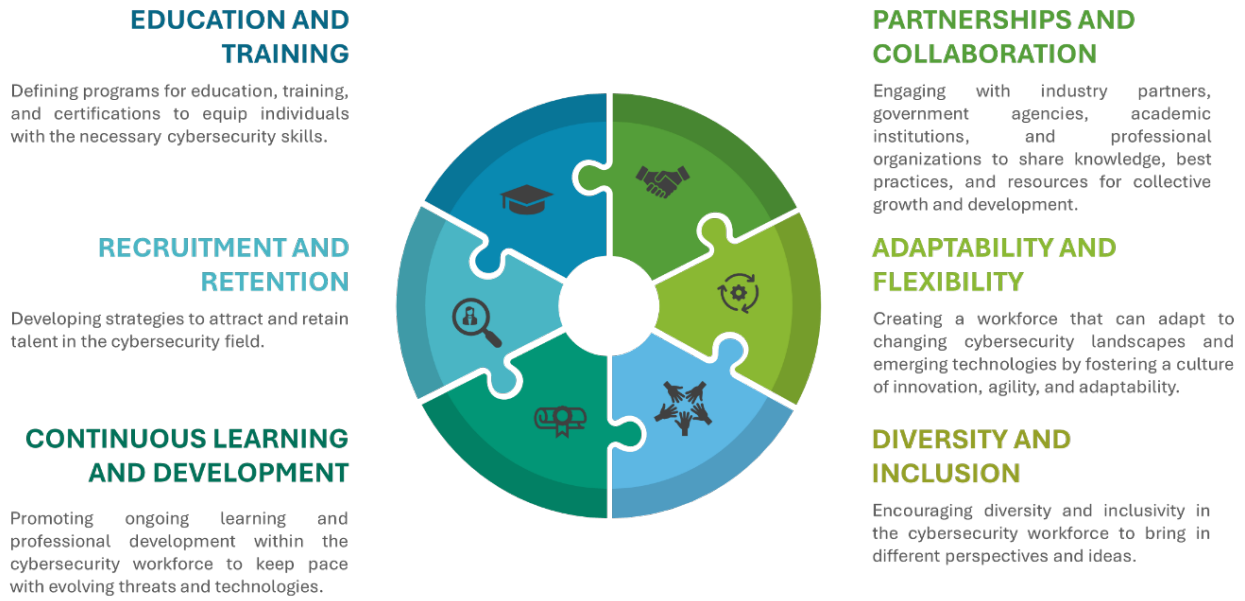


Figure 3: Six-Step Approach to meet the goals and objectives of the Hawai‘i Statewide Cyber Workforce Development Strategy

Actionable Approach for Implementation of the Cyber Workforce Development Strategy

In addition to a broad strategic vision for building and sustaining Hawai‘i’s cyber workforce, key activities to be undertaken by the State to achieve the goals and objectives of this strategy have been defined. Those activities represent the actionable steps to achieve a strong and resilient cyber workforce. Those key activities are designated in the document and further defined in Appendix A: Implementation Plan by this icon: 🔖

NICE Framework

This cyber workforce strategy also intends to lay the foundation for further, long-term integration with principles outlined in the *National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity*[11]. This includes integrating the framework's guidelines and principles into the development, implementation, and evaluation of the workforce strategy. The NICE framework provides a comprehensive blueprint for organizing and defining cybersecurity work roles, tasks, and knowledge requirements, which can be leveraged to create a robust and effective cyber workforce development strategy. The Hawai'i *Statewide Cyber Workforce Development Strategy* is organized to synchronize with best practices and principles of the NICE framework.

The following NICE principles have been incorporated into activities to be undertaken by the State of Hawai'i. As these principles are crosscutting across the *Statewide Cyber Workforce Development Strategy,* these activities are organized within the six-step strategies of Education and Training, Recruitment and Retention, Continuous Learning and Development, Partnerships and Collaboration, Adaptability and Flexibility, and Diversity and Inclusion.

1. Map Work Roles and Tasks

- **Identify Key Roles**: Use the NICE framework to identify critical cybersecurity roles needed within the organization. The framework categorizes roles into seven broad categories, such as Securely Provision, Operate and Maintain, Protect and Defend, Analyze, Collect and Operate, Investigate, and Oversight and Development.
- **Define Specific Tasks:** For each role, outline specific tasks and responsibilities. The NICE framework provides detailed descriptions of the tasks associated with each role, ensuring clarity and comprehensiveness.

2. Assess and Develop Competencies

- **Tasks, Knowledge, Skills (TKSs):** Align job descriptions and requirements with the TKSs defined in the NICE framework. This ensures that all necessary competencies are covered.
- **Competency Assessment:** Conduct regular assessments to evaluate the current skill levels of the workforce against the NICE-defined TKSs. This helps in identifying gaps and areas needing improvement.

[11] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf

3. Curriculum Development

- **Training Programs:** Develop training programs and curricula that are aligned with the NICE framework's learning objectives. This includes both foundational knowledge and specialized training for different roles.
- **Certifications and Qualifications:** Incorporate industry-recognized certifications that align with the NICE framework to validate and enhance the skills of the workforce.

4. Career Pathways and Professional Development

- **Career Mapping:** Use the NICE framework to create clear career pathways within the organization. This helps employees understand how they can progress and what skills they need to advance.
- **Continuous Learning:** Encourage a culture of continuous learning and development, utilizing the NICE framework to guide professional development plans and opportunities.

5. Recruitment and Hiring

- **Standardized Job Descriptions:** Develop standardized job descriptions based on the NICE framework to ensure consistency and clarity in recruitment.
- **Assessment Tools:** Implement assessment tools and techniques that evaluate candidates against the TKSs defined in the NICE framework.

6. Performance Management

- **Evaluation Metrics:** Establish performance metrics that are aligned with the tasks and competencies defined in the NICE framework. This ensures that performance evaluations are relevant and focused on critical areas.
- **Feedback Mechanisms:** Use structured feedback mechanisms to provide employees with clear guidance on how to improve their skills in alignment with the NICE framework.

7. Organizational Alignment

- **Strategic Integration:** Ensure that the cyber workforce strategy is integrated into the broader organizational strategy. Aligning with the NICE framework helps in creating a unified approach that is recognized and supported at all levels of the organization.
- **Policy Development:** Develop and enforce policies that support the implementation of the NICE framework within the organization, ensuring consistency and adherence to best practices.

8. Collaboration and Partnerships

- **Industry and Academia:** Collaborate with industry partners and academic institutions to align educational programs and industry needs with the NICE framework. This ensures a steady pipeline of qualified professionals.
- **Community Engagement:** Engage with the wider cybersecurity community to stay updated on the latest trends and updates to the NICE framework, ensuring that the workforce strategy remains current and effective.

By aligning a cyber workforce strategy with the NICE framework, Hawai‘i organizations can ensure that their workforce is well-prepared, their training programs are comprehensive, and their recruitment and development processes are standardized and effective. This alignment not only addresses current cybersecurity needs but also builds a foundation for future growth and adaptation in an ever-evolving field.

1. Education and Training

A well-structured training and education program is essential for supporting a cyber workforce development strategy, as it ensures that personnel possess the up-to-date skills and knowledge needed to combat evolving cyber threats. By offering targeted training programs, organizations in Hawai'i can address specific skill gaps identified in workforce assessments, thereby enhancing its overall security posture. A comprehensive training and education strategy not only equips the workforce with the necessary technical expertise but also cultivates a culture of continuous improvement and adaptability, which is vital in the ever-changing field of cybersecurity.

Upskill Existing Workforce

Upskilling the existing workforce is critical to maintaining and growing talent within the State. Effective training initiatives can alleviate staff shortages by broadening skill sets and preventing major skills gaps. Organizations that invest in continuous training programs are likely to have fewer critical skills gaps, higher levels of workforce retention, and less reliance on outsourcing.

No concerted statewide cyber training program exists in Hawai'i; however, many organizations do have training programs which cater to their internal workforce. Additionally, several nongovernmental organizations and public-private collaborations exist, such as Cyber Hawai'i, which provide training opportunities to the State's cyber workforce. However, the establishment of a collaborative, centralized statewide cyber training program is critical to building a capable cyber workforce within the State.

Activity 1.1: Establish a Statewide Cyber Training Program

Establishing a statewide cyber training program offers numerous benefits for the State's public and nongovernmental organizations. With the increasing prevalence of cyber threats, a well-trained workforce is crucial in safeguarding sensitive data and maintaining the integrity of IT systems. Employees equipped with the latest cybersecurity knowledge and skills are better prepared to identify and respond to potential threats, reducing the likelihood of breaches and ensuring the organization's defenses are effective and up to date. In terms of workforce development, a robust cyber training program contributes to employee development and retention. Offering regular training opportunities demonstrates organizational commitment to professional growth, which can increase job satisfaction and retention. Additionally, a well-trained cyber workforce can serve as a competitive advantage, positioning the State as a leader in cybersecurity and attracting top cyber talent. The development of a collaborative statewide cyber training program includes the steps outlined below.

1. **Needs Assessment:** Developing a cyber training program begins with conducting a thorough needs assessment. This initial step involves identifying the specific cybersecurity skills and knowledge gaps within your organization. By understanding the current level of cybersecurity awareness and the unique challenges faced by your staff, you can tailor the training program to address these needs effectively. Engaging with key stakeholders, including IT professionals, department heads, and employees, provides valuable insights into the areas that require focus and ensures the training program is relevant and comprehensive. The needs assessment will also identify non-technical, soft skills that provide a beneficial foundation for cybersecurity professionals.
2. **Learning Objectives:** Once the needs assessment is complete, the next step is to define clear and measurable learning objectives. These objectives should outline what participants are expected to learn and achieve by the end of the training. For instance, objectives might include the ability to recognize phishing attempts, understanding best practices for password management, or gaining proficiency in using specific security tools. Having well-defined objectives not only guides the content development but also provides a basis for evaluating the effectiveness of the training program.
3. **Training Development:** Designing the training program involves creating or selecting appropriate training materials and methods. This can include a mix of interactive virtual or in-person workshops, online modules, video tutorials, and hands-on exercises. It is essential to choose training methods that cater to different learning styles to maximize engagement and retention. Incorporating real-world scenarios and simulations can make the training more practical and relevant. Additionally, developing a structured curriculum that progressively builds on each topic ensures a coherent and comprehensive learning experience.
4. **Implementation:** Implementation of the training program requires careful planning and coordination. Scheduling the training sessions, arranging necessary resources, and selecting qualified instructors are critical components of this phase. Communication is also key; informing employees about the training program, its importance, and expectations helps in securing their commitment and participation. Providing flexible training options, such as on-demand online modules, can accommodate diverse schedules and increase accessibility. As necessary, implementation of this strategy should leverage existing training being used internally or from third-party sources.
5. **Evaluation:** Evaluation and continuous improvement are vital for the success of the cyber training program. After the training sessions, collecting feedback from participants through surveys or interviews helps assess the program's impact and identify areas for

improvement. Analyzing assessment results, such as quizzes or practical tests, can measure the effectiveness of the training in achieving its objectives. Regularly updating the training content to reflect the latest cybersecurity threats and best practices ensures the program remains current and effective.

6. **Documentation and Reporting:** Finally, documentation and reporting are essential for tracking the progress and outcomes of the training program. Keeping detailed records of attendance, assessment results, and feedback provides valuable data for ongoing improvement and accountability. Reporting the success and benefits of the training program to senior management reinforces the value of cybersecurity education and supports continued investment in this critical area. Through a well-structured and continuously evolving cyber training program, organizations can significantly enhance their cybersecurity posture and resilience.

Activity 1.2 NICE Framework Tasks, Knowledge, and Skills

Hawai'i shall undertake a statewide effort to define tasks, knowledge, and skills (TKSs) among its cyber workforce. The NICE Workforce Framework for Cybersecurity (NICE Framework, NIST Special Publication 800-181, revision 1) provides a set of building blocks for describing the TKSs that are needed to perform cybersecurity work by individuals or teams. Consistent use of the NICE Framework's building blocks enables communication at a peer level, sector level, state level, national level, or international level, which can drive innovative solutions to common challenges, lower barriers to entry for new organizations and individuals, and facilitate workforce mobility.[12]

Activity 1.3: Catalog Existing Training Opportunities

The creation of a cyber training and education program should also include leveraging existing training courses and programs within the State. This activity includes the cataloging and consolidation of existing training opportunities from government and industry organizations. A thorough review of existing courses and a centrally accessible portal will be undertaken and made available to government and nongovernment organizations.

[12] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf

Training and Education for the Non-Cyber Workforce

An effective cyber training and education program must go beyond targeting only individuals already in the cyber workforce. By reaching those outside the field, the program can address the growing demand for cybersecurity professionals and help close the skills gap. Ultimately, a successful cyber training and education program should not be limited to those already working in cybersecurity but should aim to build a diverse and skilled workforce by reaching untapped talent in adjacent fields and educational environments.

Activity 1.4: Expand Training and Education

The State, in partnership with education institutions, county governments, and industry partners, will expand training and education opportunities for those currently outside of the cyber workforce. Those training and education opportunities will focus on four areas:

1. **Career Transition for Professionals:** Many professionals in other technical fields, such as IT, software development, or engineering, possess foundational skills that can easily transfer to cybersecurity roles. A well-designed training program can introduce them to the necessary technical and non-technical aspects of cybersecurity, enabling them to pivot their careers. For instance, IT administrators who are skilled in network management could enhance their skills with cybersecurity-specific knowledge, like threat detection and incident response.
2. **Non-Technical Roles in Cybersecurity:** Not all cybersecurity jobs require deep technical knowledge. Training programs that focus on non-technical skills, such as risk management, compliance, policy development, and security awareness training, can attract individuals with backgrounds in law, business, or communication. This broadens the pool of potential cybersecurity professionals, making it accessible to a wider range of candidates.
3. **Early Education in Cybersecurity:** By promoting cybersecurity as a career path to younger audiences, such as K-12 and college students, the program can create a pipeline of future professionals. Introducing cybersecurity concepts through engaging content, practical projects, and hands-on activities helps raise awareness and interest in the field from an early age. For example, coding camps, cybersecurity competitions, and partnerships with educational institutions, such as GenCyber Hawai‘i[13], can encourage students to explore cybersecurity as a career option.

[13] https://gencyber-hi.org/

4. **Increasing Awareness of Cyber Threats:** For those not directly in the cybersecurity field, gaining basic cybersecurity awareness is crucial for maintaining digital safety in today's interconnected world. By targeting students and professionals outside the cybersecurity domain, the program fosters a culture of security-minded individuals who can recognize threats and take proactive steps to safeguard their personal and organizational data.

Promote State Education Programs

Several colleges and universities in Hawai'i offer cybersecurity programs, ranging from certificates to bachelor's and master's degrees, catering to both new students and professionals looking to advance their careers in cybersecurity. Higher education cybersecurity programs can play a significant role in attracting talent to a state and reducing the workforce gap by leveraging a combination of educational opportunities, industry partnerships, and career prospects.

Partnerships with industry and government agencies play a crucial role in attracting students. Colleges and universities that work with local companies, government agencies, and military institutions provide valuable internship opportunities and job placements for graduates. This hands-on experience gives students a competitive edge in the job market. Collaboration with cybersecurity hubs, especially in states that host significant defense contractors, military operations, or tech firms, can further entice talent. For example, Hawai'i 's proximity to Pacific military operations makes it an attractive location for students interested in defense-related cybersecurity work.

Financial incentives are another key factor. Offering scholarships, grants, and tuition assistance specifically for cybersecurity students draws talent from other regions. States with generous financial aid packages, including work-study programs and

Program Highlight:

UNIVERSITY of HAWAI'I® WEST O'AHU

The **University of Hawai'i, West Oahu** offers Bachelor of Science in Cybersecurity provides students with an advanced cybersecurity education in information security, mathematics, computer science, and computer engineering. This technical cybersecurity degree program prepares students to meet the advanced cybersecurity workforce requirements of public sector agencies and private sector enterprises. This degree program supports both four-year students at UH West Oahu and pathway students from aligned Associate Degree programs from University of Hawai'i Community Colleges.

Figure 4: https://westoahu.hawaii.edu/academics/degrees/cybersecurity/

military benefits, make education more accessible, especially for veterans and active-duty military personnel. In areas with large military populations, cybersecurity programs tailored to national security needs can draw students looking for programs that align with their military backgrounds or career goals.

Community outreach and engagement efforts further draw talent by building interest from a young age. Programs that connect with K-12 students through cyber competitions, workshops, and summer camps can inspire local talent to pursue cybersecurity education in-state. Hosting cybersecurity competitions at the college level also enhances a school's reputation, drawing students who want to compete at high levels. In addition, strong alumni networks that showcase successful graduates can attract prospective students by providing valuable connections for internships and job placements.

Activity 1.5: Promote State Education Programs

The State will coordinate with existing education programs at the K-12, college, and post-college levels to catalog and maintain a database of cybersecurity programs. The State will identify opportunities to promote these programs and integrate their students into State cybersecurity opportunities, such as seminars and exercises.

Internship Programs

Internship programs are crucial for developing Hawai‘i's cyber workforce and retaining local talent within the state. These programs offer practical experience that helps students and early-career professionals apply theoretical knowledge to real-world cybersecurity challenges. Interns engage in live projects, participate in incident response, and utilize industry-standard tools, which enhances their understanding of cybersecurity operations and prepares them for successful careers within Hawai‘i.

Internships play a significant role in nurturing local talent for Hawai‘i’s cybersecurity sector. Structured learning opportunities and mentorship help interns build a solid foundation of skills and knowledge. This approach not only equips them with essential expertise but also helps organizations identify high-potential individuals who can be cultivated for future roles. Investing in these programs ensures that local talent is developed and retained, addressing the state's need for skilled cybersecurity professionals.

Creating a direct talent pipeline through internships helps address the issue of brain drain by keeping Hawai’ians in the state. By providing meaningful work experiences and clear career pathways, these programs encourage interns to stay in Hawai‘i after graduation. Organizations can identify and recruit top-performing interns for full-time positions, which reduces recruitment

costs and ensures a steady influx of qualified candidates who are already familiar with the state's cybersecurity landscape.

Internships also address skill gaps in cybersecurity by providing practical experience that complements academic education. As the field evolves and demand for skilled professionals grows, internships help bridge the gap between theoretical knowledge and industry requirements. This preparation ensures that new professionals are well-equipped to tackle emerging cybersecurity challenges, contributing to a robust and capable local workforce.

Furthermore, internships build valuable connections between organizations and educational institutions in Hawai'i. By partnering with universities and colleges, organizations can influence curriculum development to better align with industry needs. This collaboration ensures that educational programs reflect current cybersecurity trends and technologies, creating a workforce that is well-prepared for future challenges and encouraging local talent to remain in Hawai'i.

Program Highlight:

The Hawai'i State Department of Labor & Industrial Relations Workforce Development Division has two paid internship programs available to the community. The **Hele Imua** program, shown above, is a 12-week internship opportunity for the State of Hawai'i. The purpose of this program is to provide eligible candidates exposure to various high-demand occupations in state government that may transition into gainful employment within Hawai'i's labor market.

Figure 5: https://labor.hawaii.gov/wdd/intern/hele-imua/

Internship programs are instrumental in developing and retaining Hawai'i's cybersecurity workforce. They provide practical experience, foster talent development, create a talent pipeline, address skill gaps, and strengthen industry relationships. By integrating these programs into their workforce strategies, organizations in Hawai'i can build a skilled, local cybersecurity workforce and reduce the tendency of talent to leave the state for opportunities elsewhere.

Activity 1.6: Develop Internship Programs

The State will coordinate an internship campaign targeting students from college, universities, and community colleges.

2. Recruitment and Retention

Recruitment and retention challenges for cybersecurity jobs in Hawai‘i are shaped by a complex mix of geographical, economic, and demographic factors that make it challenging for the state to build and sustain a strong cybersecurity workforce. Hawai‘i's remote location presents barriers to attracting out-of-state talent. Economically, the high cost of living in the state further complicates recruitment efforts, making it hard to compete with mainland opportunities. Demographically, the limited local talent pool, particularly in specialized technical fields like cybersecurity, creates additional strain, as the state must rely heavily on education and training programs to cultivate homegrown professionals. These factors contribute to the ongoing difficulty Hawai‘i faces in both attracting qualified candidates to fill its cybersecurity roles and retaining them in the long term. Key challenges include:

1. **Geographic Isolation:** Hawai‘i’s remote location in the Pacific Ocean makes it difficult to attract talent from the mainland United States and other regions. The cost and logistics of relocating to Hawai‘i can be prohibitive for many potential candidates.
2. **High Cost of Living:** Hawai‘i has one of the highest costs of living in the United States, driven by expensive housing, food, and utilities. This can deter potential employees from moving to the state, especially if salaries do not sufficiently offset these costs.
3. **Limited Local Talent Pool:** The local labor market in Hawai‘i is relatively small, which limits the pool of qualified candidates for specialized positions. This is particularly challenging for industries like technology and healthcare, where specific skills and experience are required.
4. **Wage Disparities:** The high cost of living necessitates higher wages, but many employers may not be able to offer competitive salaries that match those on the mainland. This disparity makes it challenging to attract and retain talent.
5. **Educational and Training Gaps:** There can be gaps in the local education and training programs, which may not fully align with the needs of certain industries, particularly those requiring advanced technical skills. This creates a reliance on importing talent from outside the state.
6. **Workforce Retention:** Retaining employees can be challenging due to the aforementioned high cost of living and limited career advancement opportunities compared to larger mainland markets. This can lead to higher turnover rates and additional recruitment challenges.

7. **Cultural Adjustment:** Candidates relocating from the mainland or other countries may face challenges in adapting to Hawai'i 's distinct cultural norms. These factors can also influence job satisfaction, employee retention, and overall performance if not properly addressed.

Recruitment

Recruitment is a critical component in establishing a strong cyber workforce in Hawai'i, where the need for skilled cybersecurity professionals is paramount. Effective recruitment strategies ensure that the workforce is composed of individuals who possess the necessary technical expertise, problem-solving abilities, and certifications required to protect sensitive information and critical infrastructure. By strategically identifying and attracting top talent, the state can build a workforce capable of addressing the complex and evolving challenges associated with cybersecurity threats.

This statewide cyber workforce strategy identifies several areas of retention where collaboration efforts across the state can help achieve this strategy's goals and objectives.

Targeted Recruitment Programs

Targeted recruitment programs are crucial in building a strong cyber workforce because they allow the state to identify and attract individuals with specific skills and expertise that align with its cybersecurity needs. These programs focus on reaching candidates with specialized knowledge in areas such as network security, threat analysis, and incident response, ensuring that the workforce is equipped to handle the unique challenges posed by cyber threats. By tailoring recruitment efforts to specific talent pools, the state can more effectively fill critical roles with professionals who are not only technically proficient but also well-versed in the particular demands of the state's cybersecurity environment. This strategic approach to recruitment enhances the overall quality and readiness of the cyber workforce, making it more capable of safeguarding Hawai'i's digital infrastructure against emerging threats. This recruitment strategy also includes:

- **Diverse Recruitment Channels:** Leverage multiple channels to attract talent, including partnerships with universities, cybersecurity bootcamps, military veteran programs, and non-profit organizations focused on underrepresented groups in technology.
- **Collaborate with Educational Institutions:** Partner with universities, technical colleges, and online education platforms to recruit students and recent graduates from cybersecurity programs. Offer internships, co-op programs, and apprenticeships to build a talent pipeline.
- **Cybersecurity Awareness Campaigns:** Launch awareness campaigns to highlight career opportunities in cybersecurity, especially targeting high school and college students, to inspire interest in the field early on.

Retention

Retention is a critical element in developing an effective cyber workforce strategy for Hawai‘i. Maintaining a stable and experienced cybersecurity team is essential for effectively addressing the complex and evolving nature of cyber threats. High retention rates help preserve institutional knowledge and expertise, reducing the risk of losing valuable insights and continuity in defending against cyber threats. Focusing on employee retention also helps mitigate the costs associated with recruitment and training. Frequent turnover leads to increased expenses and time spent on hiring new personnel, which can detract from resources needed for cybersecurity improvements. By prioritizing retention, Hawai‘i can reduce these costs and allocate more resources toward strengthening its cybersecurity capabilities. Additionally, a strong retention strategy contributes to a positive work environment and strengthens organizational culture. Employees who feel valued and see opportunities for career advancement are more likely to remain with their organizations and perform at their best. This continuity fosters a cohesive team that can collaborate effectively and respond to cybersecurity challenges with greater efficiency.

Activity 2.1: Cyber Talent Recruitment

The SLCGP CWG, via OHS, will coordinate with organizations represented in the Cyber Working Group to establish cyber workforce recruitment strategies and implementation activities. These activities will include a recruitment plan, collaboration strategies with institutions of higher education, partnerships with existing cyber awareness campaigns.

Expanding Recruitment to Non-Traditional Talent

Expanding recruitment to non-traditional talent is important for building a strong cyber workforce. This approach allows the State of Hawai‘i to tap into a wider and more diverse pool of candidates who may possess unconventional but valuable skills. Non-traditional talent, such as individuals from different industries, career changers, or those with self-taught expertise, can bring fresh perspectives and innovative problem-solving approaches to cybersecurity challenges. These candidates often have unique experiences that can contribute to addressing the complexities of cyber threats in ways that traditional pathways might overlook. By broadening recruitment efforts to include non-traditional talent, the state can enhance the creativity and adaptability of its cyber workforce, ensuring it is well-equipped to meet the evolving demands of cybersecurity. This strategy will include:

- **Upskill and Reskill Initiatives:** Actively recruit professionals from adjacent fields (e.g., IT, network administration, software engineering) and offer reskilling programs to transition them into cybersecurity roles.

- **Inclusion of Non-Traditional Candidates:** Promote diversity by recruiting individuals with non-traditional backgrounds, such as career-changers, veterans, the recently retired, and underrepresented groups, with tailored on-the-job training programs.

Activity 2.2: Non-Traditional Talent Recruitment

The SLCGP CWG, via OHS, will convene its Cyber Working Group to examine pathways for promoting recruitment of non-traditional cyber workforce talent.

Cyber Marketing Strategy

Using a marketing strategy for recruiting talent is essential in building a strong cyber workforce. A well-crafted marketing approach helps the State of Hawai'i effectively communicate its unique value proposition to potential candidates, highlighting the benefits of working in its cybersecurity sector. By leveraging targeted messaging, social media campaigns, and branding efforts, the state can attract top talent who might not otherwise consider a career in public service or cybersecurity. A strategic marketing plan can also emphasize the state's commitment to innovation, professional growth, and the impact that candidates can make in protecting critical infrastructure. This approach not only increases visibility but also enhances the appeal of cyber roles, making it easier to attract skilled professionals who are motivated to contribute to the state's cybersecurity efforts.

Program Highlight:

Founded in 2009, **ClimbHI** seeks to inspire students to finish high school and proceed to post-secondary education or employment by exposing them to future career paths and the steps necessary to achieve those goals. ClimbHI is a Hawaii-based 501(c)(3)nonprofit that focuses on three main program areas: Leadership, Exploration, Inspiration (LEI) events; the Service Excellence Certificate for high school students; and the ClimbHI Bridge online portal that connects businesses, educators and students.

Figure 6: https://climbhi.org/

Activity 2.3: Cyber Workforce Marketing

Through the SLCGP CWG and its working groups, a cyber workforce marketing strategy will be developed. This strategy will include definition of a value proposition, branding definitions, target audience identification, content development, and channel identification. These activities will be done in coordination with other State organizations responsible for marketing, traditional media, and social media.

Targeting K-12 Students

Targeting K-12 students for recruiting future talent is a proactive strategy in building a strong cyber

workforce. By engaging students early in their educational journey, the State of Hawai‘i can inspire interest in cybersecurity and develop a pipeline of skilled professionals who are well-prepared to address future challenges. Introducing cybersecurity concepts through school programs, competitions, and partnerships with educational institutions can spark curiosity and provide foundational knowledge. This early exposure not only helps students develop critical thinking and technical skills but also fosters a long-term interest in cybersecurity careers. By cultivating this interest from a young age, the state can ensure a steady supply of motivated and knowledgeable individuals who are ready to contribute to the cybersecurity field as they enter the workforce.

Activity 2.4: K-12 Marketing

Educational material will be developed targeted towards K-12 students. This material will promote cyber awareness, provide foundational cyber knowledge, and generate exposure of cybersecurity as a potential future career.

Targeting Higher Education Students

Targeting university students for recruiting future talent is a strategic approach to building a strong cyber workforce. By focusing on students who are already pursuing degrees in cybersecurity, computer science, and related fields, the State of Hawai‘i can identify and attract individuals with the technical skills and knowledge needed to address the state's cybersecurity needs. Engaging university students through internships, mentorship programs, and collaborative research projects not only provides them with hands-on experience but also helps the state build relationships with future professionals. This approach allows the state to nurture talent early in their careers, offering them pathways to employment within Hawai‘i's cybersecurity sector. By connecting with students before they enter the job market, the state can secure a pipeline of highly qualified candidates who are well-equipped to tackle emerging cyber threats.

Program Highlight:

The University of Hawai‘i IT/Cyber Leap-Start Program provides significant real-world professional experience for IT and cybersecurity students approaching graduation, and recent UH graduates who need practical work experience. Leap-Start’s goal is to improve the workforce readiness of students and graduates to successfully compete for IT and cyber employment in Hawai‘i while providing employers with much needed resources.

Figure 7: https://www.hawaii.edu/news/2022/09/28/students-leap-start-into-high-demand-it-jobs/

Activity 2.5: High Education Cyber Recruitment

The state, through OHS, will support the recruitment of higher education students through targeted outreach, awareness campaigns, and through hosting cybersecurity workshops, seminars, and guest lectures at universities, featuring experts from state agencies and industry partners. These events not only raise awareness of cybersecurity career opportunities within Hawai‘i but also allow students to network with professionals and learn about the impact they can make by joining the state’s workforce.

3. Continuous Learning and Development

Continuous education opportunities, such as certifications and advanced coursework, enable cybersecurity professionals to stay abreast of the latest technologies, threat landscapes, and regulatory requirements, which are critical for maintaining robust defenses. Moreover, these programs foster career growth and job satisfaction, aiding in the retention of top talent.

Aligning Job Roles with the NICE Framework

The State of Hawai‘i can enhance its cybersecurity continuous learning and development by aligning job roles with the National Initiative for Cybersecurity Education (NICE) Framework. The NICE Framework provides clear definitions for various cybersecurity roles, outlining the specific tasks, knowledge, skills, and abilities (TKSs) needed for each. By mapping current job roles within state agencies to the NICE Framework, Hawai‘i can establish consistency in defining continuous learning and development initiatives which map to documented skill gaps.

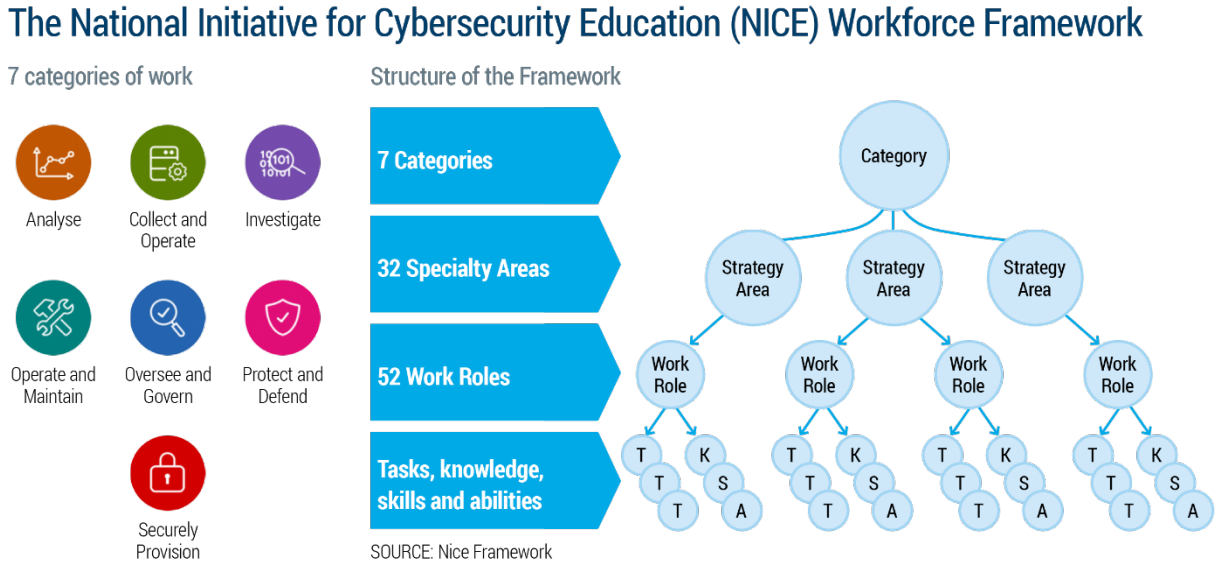


Figure 8: The NICE Framework establishes a common language that describes cybersecurity work and the knowledge and skills needed to complete that work. It is used in public and private sectors and across industries for career discovery, education, and training, and in hiring and workforce development. (https://niccs.cisa.gov/workforce-development/nice-framework)

Identifying Skill Gaps

Utilizing the NICE Framework allows the State of Hawai‘i to identify skill gaps within its cybersecurity workforce. By comparing the TKSs required for different roles with the existing skills

of employees, state agencies can pinpoint where additional development or training is necessary. This process makes it easier to address deficiencies and ensures the state's cybersecurity professionals are fully equipped to tackle emerging threats. Identifying these gaps also helps in planning targeted professional development initiatives that directly address the needs of Hawai'i 's cybersecurity workforce.

Activity 3.1: Skills-Gap Analysis

The State will initiate an annual skills-gap survey usings NICE TKSs (see Activity 1.2) to better understand current cyber workforce capabilities and skills gaps. This information will be shared with relevant public and private partners to support workforce development efforts across the state.

Designing Targeted Training and Professional Development

The NICE Framework can guide the State of Hawai'i in designing training programs that are tailored to specific cybersecurity roles within its agencies. Each role in the framework comes with detailed TKSs, which can serve as the foundation for both initial training and ongoing professional development. By aligning training programs with these competencies, Hawai'i can ensure that state employees receive relevant and up-to-date instruction. This approach ensures that cybersecurity professionals remain adaptable and capable of handling new challenges, ultimately strengthening the state's ability to safeguard its digital infrastructure.

Activity 3.2: Targeted Training and Development

the State will integrate information from the skills-gap analysis into the Statewide Cyber Training Program (see Activity 1.1) to ensure training and education efforts are aligned with known skills gaps.

Career Pathways

The NICE Framework also supports the development of clear career pathways for Hawai'i's cybersecurity workforce. By outlining the skills, tasks, and abilities required for each role, the framework helps create structured advancement opportunities for employees. Hawai'i can use this information to establish progression paths from entry-level roles to more advanced positions within state agencies. Clear career pathways encourage employee retention and development, ensuring the workforce remains engaged and motivated to grow within the organization. This structured career development supports long-term workforce sustainability.

Activity 3.3: Career Pathways Development

The State will develop, using the NICE Framework, career pathways to establish cyber career progression paths. The career pathways will be shared widely with public and private partners to support the State's cyber workforce development.

Enhancing Recruitment and Hiring Processes

Incorporating the NICE Framework into recruitment and hiring processes enables Hawai'i to clearly define the qualifications needed for each cybersecurity role. Job descriptions can be crafted based on the TKSs specified in the framework, ensuring that candidates with the appropriate skills and experience are targeted. This standardization streamlines the hiring process and helps human resource teams assess candidate suitability more effectively. By leveraging the NICE Framework, Hawai'i can improve its ability to attract and hire the right talent to fill critical cybersecurity positions across state agencies.

Activity 3.4: Informing Job Descriptions

TKSs defined in Activity 1.2 will be shared with public and private partners to ensure job descriptions match the knowledge, skills, and abilities needed to grow the State's cyber workforce.

Evaluating and Measuring Workforce Performance

The NICE Framework provides a strong foundation for evaluating and measuring the performance of Hawai'i 's cybersecurity workforce. By linking performance evaluations to the TKSs and tasks associated with each role, state agencies can establish clear and objective criteria for assessing employee performance. This approach allows for targeted feedback and ensures that performance assessments are directly related to the responsibilities and competencies required for the role. Performance metrics tied to the NICE Framework can also inform decisions about promotions, professional development, and employee retention.

Activity 3.5: Workforce Performance Measurement

The State will establish a mechanism for annually measuring the cyber workforce. This performance measurement process will establish Key Performance Indicators (KPIs), collect data across public and private partners, and communicate results across the state.

Fostering Collaboration Across Departments

The NICE Framework can help foster better collaboration between Hawai'i 's cybersecurity professionals and other departments within state agencies. Cybersecurity impacts many areas of government, and the framework's standardized language and expectations around roles and

responsibilities ensure that all teams understand their role in protecting the state's digital assets. This cross-departmental clarity promotes cooperation and coordination, helping to create a security-conscious culture throughout state government.

Improving Compliance and Risk Management

For Hawai'i , the NICE Framework is a valuable tool in meeting regulatory and compliance requirements. Many industries and sectors within the state are subject to cybersecurity regulations, and the NICE Framework helps define the roles and skills necessary to maintain compliance. By aligning the workforce strategy with the framework, Hawai'i ensures it has the right personnel in place to protect critical systems and data. This structured approach to workforce development also supports risk management efforts, enabling state agencies to better mitigate cyber risks and enhance their overall security posture.

4. Partnerships and Collaboration

The growing complexity and frequency of cyber threats require a dynamic and highly skilled cybersecurity workforce. Collaborative efforts across education, government, industry, and non-profit sectors are crucial for the continued growth and development of the cybersecurity workforce. By leveraging the strengths of each sector, these partnerships can create a sustainable talent pipeline that is capable of addressing the evolving landscape of cyber threats.

Public-private partnerships can drive workforce development by combining the strengths of government and private sector initiatives. Governments can collaborate with private organizations to launch cybersecurity awareness campaigns, skills training programs, and initiatives aimed at broadening the talent pool, such as recruiting veterans or career-changers. These partnerships can also fund research and development efforts, leading to innovative solutions that address current and future cybersecurity challenges. Joint exercises and simulations allow both public and private entities to train cybersecurity professionals in responding to real-world threats, enhancing their readiness and expertise. Through education, public-private initiatives, international cooperation, industry collaboration, and community involvement, the cybersecurity workforce can grow in both expertise and capacity, ensuring that organizations are well-prepared to meet the challenges of the digital age.

Program Highlight:

CYBER HAWAII

CyberHawaii organizes an Education and Workforce Development Committee to, "promote a deeper awareness and understanding of cyber threats specific to Hawai'i and ensure that we are developing and accelerating educational opportunities from K-12 into higher education & students are job ready upon graduation and successful in securing cybersecurity job in Hawai'i."

CyberHawaii also hosts a career site that job candidates can use to submit their resumes to hiring managers in the Department of Defense (DoD) and to its major contractors. Jobs opportunities in intelligence, IT, cybersecurity, and data science are typical in Hawai'i.

Figure 9: https://www.cyberhawaii.org/committees/education-workforce-development/

Education and Industry Partnerships

Public-private partnerships with universities in Hawai'i can bolster cyber workforce development by aligning academic programs with industry needs. Collaboration with private sector companies allows Hawai'i's universities to shape curricula that address current cybersecurity challenges and

incorporate the latest technologies. This ensures that students receive an education directly applicable to the demands of the cybersecurity job market within the state. By integrating industry expertise, universities in Hawai‘i can offer programs that produce graduates well-prepared to enter and excel in the workforce.

These partnerships provide students with essential practical experience, a critical component of cybersecurity education. Sponsorship of internships, cooperative education programs, and research projects by private companies offer students opportunities to apply their knowledge in real-world settings. This hands-on experience reinforces classroom learning and helps students develop the problem-solving skills necessary in the rapidly evolving field of cybersecurity. Working alongside industry professionals, students gain insights into the latest tools, strategies, and threats, making them more competitive candidates upon graduation.

For private companies operating in Hawai‘i, partnering with local universities is a strategic way to identify and nurture top talent early in their careers. Companies can engage with students through guest lectures, workshops, and career fairs, establishing relationships that may lead to future employment opportunities within the state. These partnerships enable the development of specialized training programs tailored to address specific skills gaps identified by the industry, ensuring that Hawai‘i’s cybersecurity workforce is equipped to handle emerging threats.

Public-private partnerships also drive innovation in cybersecurity through joint research initiatives. By pooling resources and expertise, Hawai‘i’s universities and private sector companies can explore new approaches to cybersecurity challenges. This collaboration advances the field and allows students to contribute to cutting-edge research, enhancing their skills and employability in Hawai‘i's growing cybersecurity sector. Additionally, internships and apprenticeship programs provide students with valuable hands-on experience, bridging the gap between theoretical learning and practical application. Partnerships can also result in certification programs, ensuring that graduates are equipped with industry-recognized credentials that meet current cybersecurity standards.

Activity 4.1: Public-Private Cyber Workforce Events

The State, through OHS, will establish regular public-private partnership events to promote cyber workforce development efforts. These events will be determined, planned, and executed through OHS and could include cyber workforce summits, job fairs, industry days, and similar events. These events will be broadly marketed across public, private, and education sectors. Additionally, the OHS will review existing events to promote cyber workforce efforts, to include activities such as adding workforce development topics to event agendas and inviting cyber workforce development partners.

Small Business Partnerships

Partnerships with small businesses are essential for building a robust cyber workforce in Hawai‘i. Small businesses frequently encounter unique cybersecurity challenges that require innovative solutions, offering a dynamic environment where employees can gain practical experience and develop specialized skills. By collaborating with small businesses, educational institutions, and training programs in Hawai‘i can tailor curricula to address the real-world needs of these companies, ensuring that graduates are well-prepared to enter the cybersecurity workforce.

Small businesses also provide valuable opportunities for internships, apprenticeships, and entry-level positions, allowing individuals to gain hands-on experience in cybersecurity. These positions offer a direct pathway for students and new professionals to start their careers, with the advantage of exposure to a diverse range of cybersecurity issues. The personalized training and mentorship available in small business environments can accelerate the development of essential skills and knowledge.

Additionally, small businesses can partner with government agencies and educational institutions to create community-based cybersecurity initiatives. These initiatives focus on local workforce development, ensuring that cybersecurity professionals are trained to meet the specific needs of Hawai‘i’s communities. By participating in these partnerships, small businesses contribute to shaping the next generation of cybersecurity experts and

Program Highlight:

Cybersafe Hawaii

Cyber Safe Hawaii is a collaborative effort led by the State of Hawaii Department of Business Economic Development and Tourism and community resource partners to highlight the importance of cybersecurity for small businesses. Cyber Safe Hawaii provides technical assessments, cyber awareness training, and penetration testing to eligible small businesses.

Figure 10: https://cybersafehawaii.org/

Program Highlight:

HAWAI‘I SBDC SMALL BUSINESS DEVELOPMENT CENTER

The **Hawai‘i Small Business Development Center** provides professional business advice, research and training to business owners and new entrepreneurs in order to promote growth, innovation, productivity and management improvement. To accomplish these objectives, we link federal, state and local resources, the educational community and the private sector to meet the needs of Hawai‘i’s businesses.

Figure 11: https://cybersafehawaii.org/

addressing their own security needs, enhancing the overall resilience and capability of Hawai'i's cyber workforce.

Activity 4.2: Small Business Collaboration

The State will coordinate with programs within the state that promote small businesses, such as Cyber Safe Hawai'i and the Hawai'i Small Business Development Center, to identify areas for collaboration in building the State's cyber workforce.

National and International Collaboration

Global partnerships offer access to a broader talent pool and enable the sharing of critical knowledge and best practices. By fostering international collaboration, organizations can recruit cybersecurity professionals from diverse regions, allowing for a more comprehensive approach to addressing global cyber threats. Furthermore, international information-sharing networks can be established to disseminate threat intelligence and emerging trends, ensuring that cybersecurity professionals are well-informed and prepared to handle evolving risks. This global approach to workforce development enhances adaptability and ensures that expertise is shared across borders.

Activity 4.3: National Collaboration

OHS will maintain its active and ongoing collaboration through the National Governor's Association's Governors' Cybersecurity Policy Advisors Network.

Activity 4.4: International Collaboration

OHS will continue to engage in the Critical Infrastructure Cybersecurity Workshop series sponsored through the US Department of Defense's Indo-Pacific Command. The mission of that forum is "To improve cybersecurity posture of Critical Infrastructure through collaborative information exchanges between the United States, allies, and partners operating in the Indo-Pacific region.

Corporate and Tech Industry Collaboration

Within the tech industry, partnerships between corporations can support the development of a more skilled and experienced cybersecurity workforce. Companies can participate in talent exchange programs, allowing cybersecurity professionals to gain experience in different corporate environments, broadening their skill sets. Collaborative initiatives such as hackathons, bug bounty programs, and cybersecurity challenges offer professionals opportunities to solve

real-world problems while fostering innovation. Joint efforts to develop cybersecurity tools and technologies also provide professionals with practical experience in creating solutions, further enhancing their technical capabilities.

Activity 4.5: Corporate and Tech Industry Collaboration

OHS will continue to maintain its active participation in and leverage the ongoing efforts of the Information Technology Sector Partnership led by the Hawaii Chamber of Commerce, state Department of Labor and Industrial Relations.

Non-Profit and Community Involvement

Non-profit organizations play a key role in promoting cybersecurity workforce development, particularly by focusing on outreach and inclusion. By partnering with educational institutions, corporations, and local communities, non-profits can introduce underrepresented groups to the field of cybersecurity. These partnerships often result in mentorship programs, where experienced professionals guide and support emerging talent, and outreach initiatives that raise awareness of cybersecurity career opportunities. Such efforts ensure that workforce development is inclusive, providing access to cybersecurity training and resources to a wider range of individuals.

Existing non-profit and community organizations in Hawai‘i provide collaboration opportunities to support the State’s cyber workforce development activities. The Hawai‘i Workforce Funders Collaborative is one example of a community organization focused on general workforce development efforts which could be used to promote cyber career pathways.

Program Highlight:

Hawai‘i Workforce Funders Collaborative

Hawai‘i Workforce Funders Collaborative was launched in partnership by HMSA, Harold K.L. Castle Foundation, The Harry and Jeanette Weinberg Foundation and the Hawai‘i Community Foundation to strengthen partnerships and systems to provide equitable access to quality, living wage jobs for Hawai‘i residents. The organization works across the public, private, and nonprofit sectors to implement workforce equity best practice and to educate and align philanthropic foundations on emerging narratives and opportunities to support Hawai‘i workers.

Figure 12: https://cybersafehawaii.org/

Activity 4.6: Non-Profit and Community Collaboration

The State will create a registry of non-profit and community organizations which could serve as force multipliers for cyber workforce development efforts. The State will collaborate with these

organizations to identify opportunities for partnerships. When appropriate, the State will use this database to invite relevant partners to state-hosted events with the intent of promoting cyber workforce development activities.

Cyber Collaboration with Existing State Programs

Several State government workforce development programs exist. These programs focus on general workforce development activities; however, with collaborative efforts these programs could also support the development of the State's cyber workforce. For example, the Hawai'i Department of Labor and Industrial Relations Workforce Development Division provides the following core services and programs to job seekers and employers:

1. Free job referral and search assistance for both job seekers and employers.
2. Develop and maintain partnerships with private and public sector stakeholders to meet various emerging trends, advancements in technology and other issues facing our economy.
3. Collaborate with educators, employers, and labor unions to identify basic skills of all workforce entrants.
4. Provide consultative and support services to both employers and laid-off workers in times of financial trouble.[14]

Program Highlight:

State of Hawaii
Workforce Development Division

The Workforce Development Division (WDD) is a part of the Hawaii State Department of Labor and Industrial Relations and provides services and resources to job seekers and employers in the state.

WDD connects job seekers to American Jobs Center Hawaii, Hele Imua—the State of Hawaii Internship Program, HireNet Hawaii, and other resources. WDD provides services to employers, such as apprenticeships, Employment and Training Fund, Work Opportunity Tax Credit, and services for military veterans.

Figure 13: https://labor.hawaii.gov/wdd/

Activity 4.7: Collaboration with Existing State-Led Programs

OHS will establish a connection with the State Workforce Development Division and any other relevant programs managed by State agencies to identify opportunities for collaboration.

[14] https://labor.hawaii.gov/wdd/about-us/

5. Adaptability and Flexibility

Adaptability and flexibility are crucial for developing a cyber workforce capable of responding to the fast-changing nature of cyber threats. The cyber landscape is dynamic, with new vulnerabilities, attack vectors, and malware constantly emerging. A static workforce with rigid skill sets will struggle to effectively counter these evolving threats. Professionals who are adaptable can quickly learn and apply new tools, techniques, and strategies, ensuring they stay ahead of malicious actors and maintain strong organizational defenses.

Technological advancements also highlight the need for flexibility. The rise of technologies such as artificial intelligence, blockchain, quantum computing, and the Internet of Things (IoT) presents new challenges in cybersecurity. A flexible workforce is more likely to engage in continuous learning, which is essential to understanding and securing emerging technologies. As organizations adopt new tech solutions, cybersecurity professionals must be able to quickly acquire the skills needed to protect these innovations from potential risks.

In addition, cybersecurity professionals need to be adaptable to working across diverse industries, each with their own specific threats and regulatory requirements. From healthcare to finance, sectors vary in the type and severity of risks they face, as well as the compliance standards they must follow. Flexible professionals can tailor security strategies based on the unique demands of the industry they serve, ensuring both operational effectiveness and regulatory compliance.

The regulatory environment itself is continually evolving as governments and industry update cybersecurity laws and standards to address emerging risks and privacy concerns. A workforce that demonstrates adaptability is essential to ensure compliance with these changing regulations. Cybersecurity professionals must be able to integrate new regulatory requirements into their practices quickly and efficiently to avoid non-compliance penalties and potential security gaps.

Adaptability fosters innovation and problem-solving, both of which are vital in cybersecurity. The field often involves complex decision-making and requires quick responses to unforeseen challenges. Professionals who are flexible in their approach can think critically and develop creative solutions to address new threats or vulnerabilities, ensuring that organizations remain secure even when faced with unprecedented risks.

The demand for cybersecurity talent frequently exceeds supply, creating skills gaps within organizations. Flexibility in career development and training is necessary to address this issue. By fostering adaptability within their workforce, organizations can help employees upskill or reskill as needed, enabling them to shift roles, take on new responsibilities, and meet evolving organizational demands.

Cross-Training and Role Rotation

Cross-training and role rotation are essential in cyber workforce development because it equips employees with a broad range of skills, making them more versatile and adaptable to various cybersecurity challenges. Cybersecurity threats are constantly evolving and having a workforce that can handle multiple aspects of security, such as network defense, incident response, and threat analysis, ensures that the organization is better prepared to respond to different types of attacks. Employees trained in diverse areas of cybersecurity can quickly shift roles as needed, enhancing the organization's overall resilience.

Cross-training and role rotation also foster collaboration and knowledge-sharing among team members. When employees have a deeper understanding of each other's responsibilities, it creates a more cohesive team that can work together more effectively during complex incidents. This mutual understanding reduces bottlenecks and improves communication, leading to quicker and more efficient responses to cybersecurity threats.

Cross-training and role rotation also enhance career development and retention. Employees who are given opportunities to learn new skills and expand their knowledge are more likely to feel engaged and motivated in their roles. Offering cross-training shows a commitment to employee growth, which can increase job satisfaction and reduce turnover. A well-rounded cyber workforce not only benefits the organization by increasing its security capabilities but also contributes to a more fulfilling career path for individuals.

Activity 5.1: Develop Cross-Functional Expertise

The State will Implement cross-training initiatives that expose employees to different cybersecurity domains, such as incident response, penetration testing, risk management, and cloud security to broaden employee skill sets, making them more versatile and capable of shifting focus when needed.

Activity 5.2: Create Role Rotation Programs

The State will create opportunities for cybersecurity professionals to rotate between different roles within organizations. This enables them to develop a deeper understanding of various security functions, enhancing their ability to adapt to new challenges or responsibilities as they arise.

Adaptability in Compliance and Regulatory Management

Adaptability in compliance and regulatory management is essential in cyber workforce development as cybersecurity regulations and standards are constantly changing. As new technologies emerge and cyber threats evolve, government and industry frequently update

compliance requirements to address new risks. Cyber professionals must be able to quickly understand and implement these changes to ensure their organizations remain compliant. Fostering adaptability in this area ensures that the workforce can keep pace with shifting regulatory landscapes and avoid penalties or breaches related to non-compliance.

Being adaptable in compliance also enables cyber professionals to tailor security practices to meet both global standards and local regulatory requirements. Different critical infrastructure sectors and industries may have specific compliance frameworks, such as HIPAA for healthcare or requirement from the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). Adaptability allows the cyber workforce to effectively navigate these complexities and apply appropriate security controls based on the specific regulatory context. This flexibility ensures that organizations can meet diverse compliance needs without compromising their security posture.

Adaptability in compliance and regulatory management encourages a proactive approach to cybersecurity. Employees who are trained to adjust quickly to new regulations are more likely to anticipate future changes and prepare for them in advance. This readiness helps organizations stay ahead of emerging threats and avoid costly last-minute changes. It also fosters a culture of continuous improvement, where the cyber workforce is constantly looking for ways to enhance security practices in line with evolving regulatory requirements.

Activity 5.3: Create Regulatory Update Briefings

The State will develop a formal process for regularly updating cybersecurity professionals on changes in compliance standards and legal regulations. This can be in the form of quarterly briefings, regular newsletters, or meetings that focus on new developments in cybersecurity laws, regulations, and compliance.

Activity 5.4: Implement Compliance Training Programs

The State will provide specific training sessions on integrating new regulations into security practices, ensuring the workforce is both knowledgeable and adaptable in applying these changes across the organization.

Monitor Adaptability

Monitoring adaptability in cyber workforce development is crucial because the cybersecurity landscape is constantly evolving. By monitoring adaptability, the State can assess whether their workforce is capable of responding effectively to these changes. This helps ensure that employees remain current with industry trends and are equipped to implement new tools and strategies to protect the organization against emerging threats.

Tracking adaptability also helps identify gaps in skills and knowledge within the team. Monitoring how well employees adapt allows organizations to provide targeted development opportunities, ensuring that the entire workforce stays aligned with the latest cybersecurity practices.

Monitoring adaptability also helps create a culture of continuous learning and innovation. When organizations actively assess and encourage adaptability, employees are more likely to embrace new challenges and seek out opportunities for growth. This mindset strengthens the overall resilience of the cyber workforce, making the team better prepared to tackle unexpected challenges and shifts in the cybersecurity environment.

Activity 5.5: Conduct Regular Skill Assessments

Aligned with Activity 3.1 Skills-Gap Analysis, the State will periodically evaluate the skills and adaptability of the workforce through assessments or simulations. This helps identify gaps and areas for development, enabling targeted upskilling efforts.

Activity 5.6: Gather Feedback for Continuous Improvement

The State will collect feedback from employees on the effectiveness of training, role rotation, and other adaptability programs. Use this data to refine the strategy and make adjustments to better support flexibility in the workforce.

6. Diversity and Inclusion

Diversity and inclusion are essential in building a strong and resilient cyber workforce. A diverse team brings a broader range of perspectives, which is crucial in addressing the global nature of cyber threats. Cybersecurity threats come from a wide variety of actors across different regions, and a workforce with diverse backgrounds, cultures, and experiences can approach these threats from multiple angles. This variety of viewpoints allows for more innovative and effective strategies for identifying vulnerabilities and developing comprehensive security solutions. Diversity and inclusion are not only social imperatives but strategic advantages in the cybersecurity field. They lead to better problem-solving, innovation, collaboration, and responsiveness while helping address the talent shortage and fostering trust with stakeholders. By building diverse and inclusive cybersecurity teams, organizations can develop stronger, more adaptable defenses against the constantly changing cyber threat landscape.

Innovation and Creativity

Innovation and creativity, both critical in the cybersecurity field, are also fostered through diversity. As the industry faces constant change and new threats, having teams with diverse educational backgrounds and professional experiences leads to creative problem-solving and agile responses. A homogenous team may fall into routine thinking, while a diverse team is more likely to approach problems from unique perspectives, resulting in innovative solutions to complex cybersecurity challenges. In a field where adaptability is key, diversity strengthens an organization's ability to respond to ever-evolving threats.

Addressing the Workforce Gap

The current talent shortage in cybersecurity is another reason why diversity and inclusion are important. The demand for skilled cybersecurity professionals often exceeds supply, leaving many critical positions unfilled. By expanding recruitment efforts to underrepresented groups, such as women, racial minorities, veterans, and those from non-traditional career paths, organizations can tap into a broader pool of talent. This not only helps address the skills gap but also strengthens the overall cyber workforce, bringing in varied expertise and perspectives that may otherwise be overlooked.

Increased Collaboration

In addition to improving technical capabilities, diversity and inclusion can enhance team collaboration. Inclusive work environments where employees feel valued and respected

encourage better communication and collaboration—resulting in higher retention rates. When team members from diverse backgrounds feel empowered to share their ideas, organizations benefit from a wider range of solutions and avoid the risk of groupthink. Inclusive teams tend to be more open, dynamic, and willing to explore unconventional approaches, which is critical in a field where flexibility and innovation are required to stay ahead of threats.

Diverse Perspectives

A diverse cyber workforce is also better positioned to understand and serve a global and diverse user base. Different demographic groups may have varying security needs, preferences, and concerns, particularly regarding privacy and access to digital services. A team that reflects this diversity is more likely to understand and address these unique challenges, ensuring that security measures are both effective and inclusive for all users. This creates a more secure environment for customers, partners, and clients from different backgrounds and regions.

Social Trust

Fostering diversity and inclusion enhances an organization's trust and reputation. In today's business landscape, where social responsibility is increasingly important, organizations that prioritize diversity are seen as more ethical and socially conscious. This commitment to diversity not only builds trust with external stakeholders but also makes the organization more attractive to top talent, strengthening the workforce over the long term.

Activity 6.1: Diversity and Inclusion Collaboration

OHS will engage the State Equal Employment Opportunity Office to collaborate on diversity and inclusion principles in all activities related to the *Statewide Cyber Workforce Development Strategy*.

Performance Metrics

Performance metrics are essential for the State of Hawai‘i in developing an effective strategy to grow its cyber workforce. These metrics provide measurable insights into the success of workforce development initiatives, such as certification completion rates, training effectiveness, or time to hire. Establishing clear key performance indicators (KPIs) allows the State to assess progress toward workforce goals and ensure that current efforts are driving results. Metrics help identify areas where adjustments may be necessary, ensuring that initiatives are optimized for success and aligned with Hawai‘i ’s specific cybersecurity needs. By providing data-driven insights into progress, skill gaps, resource allocation, and strategic needs, these metrics allow Hawai‘i to develop a workforce that is adaptable, skilled, and prepared for the cybersecurity challenges unique to the state. Integrating performance metrics ensures that Hawai‘i is building a resilient and future-proof cyber workforce that can safeguard the state’s digital infrastructure.

In Hawai‘i ’s evolving cybersecurity landscape, performance metrics play a critical role in identifying skill gaps within the workforce. As cyber threats continue to evolve, state agencies must ensure their teams are equipped with the skills necessary to address these emerging challenges. Regular assessment of employees’ skills using these metrics highlights areas where additional training or development is required. This targeted approach helps the state’s workforce stay prepared, enabling Hawai‘i to proactively address cybersecurity vulnerabilities and respond effectively to complex threats.

Performance metrics are also key to optimizing resource allocation in cyber workforce development. The state invests significant resources in training, recruitment, and professional development programs. Tracking which initiatives yield the best results allows Hawai‘i to direct resources more efficiently. Programs that consistently lead to improved employee performance and retention can receive additional support, while less effective initiatives can be restructured or scaled back. This data-driven approach ensures that public resources are maximized, providing the highest return on investment for the state's cybersecurity capabilities.

Performance metrics support strategic decision-making by offering valuable insights into workforce trends over time. Hawai‘i ’s state agencies can analyze data related to certifications, turnover rates, and recruitment success to inform decisions about future workforce needs. This analysis helps forecast potential talent shortages, identify emerging demands, and ensure that the workforce is prepared to meet Hawai‘i ’s long-term cybersecurity challenges. Metrics lay the foundation for a sustainable and future-ready cybersecurity strategy that aligns with the state’s unique needs.

Accountability and continuous improvement are fostered through performance metrics. Setting clear goals and benchmarks within the state's cyber workforce creates an environment where employees and teams are held accountable for their performance. Regular monitoring of these metrics ensures that state employees remain engaged in their professional development and adapt to new challenges. This focus on continuous improvement keeps Hawai'i 's workforce agile and prepared to respond to the rapidly changing cybersecurity landscape.

Performance metrics also play a role in enhancing employee engagement and retention within Hawai'i 's cyber workforce. Employees who see their development measured and linked to clear career progression paths are more likely to feel motivated and valued. Metrics tied to promotions, salary increases, or skill development can foster a sense of achievement and commitment, improving employee satisfaction and loyalty. This helps the state retain top talent while continuously building the capabilities of its cyber workforce to protect Hawai'i 's public sector infrastructure.

To effectively measure the performance of a cyber workforce strategy, organizations can use a variety of metrics that assess different aspects of workforce capabilities, development, and outcomes. The SLCGP CWG, via OHS, will be responsible for defining, tracking, monitoring, and reporting performance metrics related to the *Statewide Cyber Workforce Development Strategy*. Proposed performance metrics include:

1. Recruitment Metrics:
    - Time to Fill Positions: Measures the average time taken to fill cybersecurity roles from job posting to hiring.
    - Offer Acceptance Rate: The percentage of job offers accepted by candidates.
    - Source of Hire: Tracks the effectiveness of different recruitment channels (e.g., job boards, referrals, educational institutions).
2. Training and Development Metrics:
    - Certification Completion Rate: The percentage of employees who complete relevant cybersecurity certifications (e.g., CISSP, CISM, CEH).
    - Training Participation Rate: The proportion of the workforce participating in ongoing cybersecurity training programs.
    - Skills Assessment Scores: Pre- and post-training assessment scores to measure improvements in cybersecurity knowledge and skills.
3. Retention Metrics:

- Employee Turnover Rate: The rate at which cybersecurity professionals leave the organization within a specific period.
- Employee Satisfaction: Measured through surveys assessing job satisfaction and engagement levels among cybersecurity staff.
- Career Progression: Tracking internal promotions and lateral moves within the cybersecurity team.

4. Workforce Assessment Metrics:
    - Number of state organizations contributing to annual cyber workforce development surveys
5. Diversity and Inclusion Metrics:
    - Diversity in Hiring: The percentage of hires from underrepresented groups in cybersecurity roles.
    - Inclusion Scores: Employee survey results reflecting the inclusiveness of the work environment.

By monitoring these metrics, the State of Hawai‘i can evaluate the effectiveness of its cyber workforce strategy, identify areas for improvement, and make informed decisions to strengthen their cybersecurity posture.

Appendix A: Implementation Plan

The Implementation Plan creates an actionable path forward for achieving the goals and objectives defined in the Cyber Workforce Strategy. The strategy includes several 'activities' which are aligned to one or more goals and objectives. These activities operationalize the steps needed to create and sustain a strong, resilient cyber workforce in the State. The Implementation Plan, and the activities listed within it, are overseen by the SLCGP CWG, which is responsible for ensuring activities are initiated and followed through to completion.

Strategy	Aligned Goal(s)	Aligned Objective(s)	Workforce Activity	State Lead(s)	Initiation Timeframe
Strategy 1: Education and Training	1 2 3 4	1 2 3 4 5 6	Activity 1.1 Establish a Statewide Cyber Training Program	OHS, ETS	6 months
Strategy 1: Education and Training	1 2 3 4	1 2 3 4 5 6	Activity 1.2 NICE Framework Tasks, Knowledge, and Skills	OHS, ETS	12 months
Strategy 1: Education and Training	1 2 3 4	1 2 3 4 5 6	Activity 1.3: Catalog Existing Training Opportunities	OHS	2 months
Strategy 1: Education and Training	1 2 3 4	1 2 3 4 5 6	Activity 1.4: Expand Training and Education	OHS, Cybersecurity Working Group	18 months

Strategy 1: Education and Training	1 2 3 4	1 2 3 4 5 6	Activity 1.5: Promote State Education Programs	OHS	6 months
Strategy 1: Education and Training	1 2 3 4	1 2 3 4 5 6	Activity 1.6: Develop Internship Programs	OHS, DLIR	12 months
Strategy 2: Recruitment and Retention	1 2 3 4	1 2 3 4 5 6	Activity 2.1: Cyber Talent Recruitment	OHS, Cybersecurity Working Group	6 months
Strategy 2: Recruitment and Retention	1 2 3 4	1 2 3 4 5 6	Activity 2.2: Non-Traditional Talent Recruitment	OHS, Cybersecurity Working Group	12 months
Strategy 2: Recruitment and Retention	1 2 3 4	1 2 3 4 5 6	Activity 2.3: Cyber Workforce Marketing	OHS, Cybersecurity Working Group	12 months
Strategy 2: Recruitment and Retention	1 2 3 4	1 2 3 4 5 6	Activity 2.4: K-12 Marketing	OHS, DOE, HAIS	18 months
Strategy 2: Recruitment and Retention	1 2 3 4	1 2 3 4 5 6	Activity 2.5: High Education Cyber Recruitment	OHS, UH, HPU	18 months

Strategy 3: Continuous Learning and Development	1 2 3 4	1 2 3 4 5 6	Activity 3.1: Skills-Gap Analysis	OHS, Cybersecurity Working Group	6 months
Strategy 3: Continuous Learning and Development	1 2 3 4	1 2 3 4 5 6	Activity 3.2: Targeted Training and Development	OHS, ETS. IT Sector Partnership	12 months
Strategy 3: Continuous Learning and Development	1 2 3 4	1 2 3 4 5 6	Activity 3.3: Career Pathways Development	OHS, ETS. IT Sector Partnership	12 months
Strategy 3: Continuous Learning and Development	1 2 3 4	1 2 3 4 5 6	Activity 3.4: Informing Job Descriptions	OHS, DHRD	12 months
Strategy 3: Continuous Learning and Development	1 2 3 4	1 2 3 4 5 6	Activity 3.5: Workforce Performance Measurement	OHS, DHRD	18 months
Strategy 4: Collaboration and Partnerships	1 2 3 4	1 2 3 4 5 6	Activity 4.1: Public-Private Cyber Workforce Events	OHS, Cybersecurity Working Group	6 months
Strategy 4: Collaboration and Partnerships	1 2 3 4	1 2 3 4 5 6	Activity 4.2: Small Business Collaboration	OHS, Cybersecurity Working Group	6 months

Strategy 4: Collaboration and Partnerships	1 2 3 **4**	**1** 2 3 4 5 6	Activity 4.3: National Collaboration	OHS	6 months
Strategy 4: Collaboration and Partnerships	1 2 3 **4**	**1** 2 3 4 5 6	Activity 4.4: International Collaboration	OHS	6 months
Strategy 4: Collaboration and Partnerships	1 2 3 **4**	**1** 2 3 4 5 6	Activity 4.5: Corporate and Tech Industry Collaboration	OHS, ETS	6 months
Strategy 4: Collaboration and Partnerships	1 2 3 **4**	**1** 2 3 4 5 6	Activity 4.6: Non-Profit and Community Collaboration	OHS	6 months
Strategy 4: Collaboration and Partnerships	1 2 3 **4**	**1** 2 3 4 5 6	Activity 4.7: Collaboration with Existing State-Led Programs	OHS, DLIR	6 months
Strategy 5: Adaptability and Flexibility	**1** 2 **3** 4	**1** **2** 3 4 5 6	Activity 5.1: Develop Cross-Functional Expertise	OHS, ETS	12 months
Strategy 5: Adaptability and Flexibility	**1** 2 **3** 4	**1** **2** 3 4 5 6	Activity 5.2: Create Role Rotation Programs	OHS, ETS	12 months

Strategy 5: Adaptability and Flexibility	1 2 3 4	1 2 3 4 5 6	Activity 5.3: Create Regulatory Update Briefings	OHS, Cybersecurity Working Group	6 months
Strategy 5: Adaptability and Flexibility	1 2 3 4	1 2 3 4 5 6	Activity 5.4: Implement Compliance Training Programs	OHS, ETS	18 months
Strategy 5: Adaptability and Flexibility	1 2 3 4	1 2 3 4 5 6	Activity 5.5: Conduct Regular Skill Assessments	OHS, ETS	18 months
Strategy 5: Adaptability and Flexibility	1 2 3 4	1 2 3 4 5 6	Activity 5.6: Gather Feedback for Continuous Improvement	OHS, ETS	18 months
Strategy 6: Diversity and Inclusion	1 2 3 4	1 2 3 4 5 6	Activity 6.1: Diversity and Inclusion Collaboration	OHS, DLIR	6 months

Appendix B: Strategy Maintenance

Maintaining and updating this document is essential to ensure its relevance and accuracy. Regular reviews should be conducted to incorporate any changes in policies, procedures, or relevant information. Updates should reflect the latest industry standards, best practices, and organizational developments. Any modifications must be clearly documented, with version control mechanisms in place to track changes over time. Stakeholders should be informed promptly of significant updates to ensure consistent and informed application of the document's guidelines.

#	Document Version	Revision Date	Revision Notes
0.1	First Draft	09/26/2024	First draft reviewed by Cyber Working Group
0.2	Second Draft	10/31/2024	Second draft reviewed by OHS

Appendix C: Acronyms

Acronym	Definition
CIRCIA	Cyber Incident Reporting for Critical Infrastructure Act of 2022
CISA	Cybersecurity and Infrastructure Agency
DBEDT	Department of Business, Economic Development, and Tourism
DHS	Department of Homeland Security
DHS	Hawai‘i Department of Human Services
DOE	Hawai‘i Department of Education
DOH	Hawai‘i Department of Health
DOT	Hawai‘i Department of Transportation
ESF	Essential Support Function
ETS	Enterprise Technology Services, Office of
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
HSEO	Hawai‘i State Energy Office
HING	Hawai‘i National Guard
HSFC	Hawai‘i State Fusion Center
IT	Information Technology
IoT	Internet of Things
KPI	Key Performance Indicator
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
OHA	Office of Hawai’ian Affairs
OHS	Hawai‘i Office of Homeland Security
OT	Operational Technology
SLCGP	State and Local Cybersecurity Grant Program
TKS	Tasks, Knowledge, Skills
UH	University of Hawai‘i
U.S.	United States
USSS	United States Secret Service
WDD	Workforce Development Division, State of Hawai‘i

Appendix D: Stakeholders and Contributors

This section lists stakeholders and contributors who either have already contributed to the development of the Hawai'i Statewide Cybersecurity Strategy or who will have a role in overseeing its implementation. This list is broken down into the following groups and is not all inclusive of stakeholders who will be involved in planning and/or implementation efforts:

- Federal Partners
- Industry Partners
- State Partners
- County / Local Partners
- Higher Education Institutions

Federal Partners

Coast Guard, U.S. (USCG)

The USCG Cyber Command supports cybersecurity operations in the state by defending Coast Guard cyberspace, enabling Coast Guard operations, and protecting the Maritime Transportation System (MTS).[15]

Cybersecurity and Infrastructure Security Agency, U.S. (CISA)

CISA operates under DHS and is responsible for strengthening cybersecurity and infrastructure protection across all levels of government, coordinating cybersecurity programs within the U.S., and improving the government's cybersecurity protections against private and nation-state hackers[16].

Federal Bureau of Investigation, U.S. (FBI):

The FBI is the lead federal agency for investigating cyber-attacks and intrusions. They collect and share intelligence and engage with victims while working to unmask those committing malicious cyber activities. The FBI will work closely with state partners in the event of a cyber-attack to support investigations.[17]

[15] https://www.dco.uscg.mil/Our-Organization/CGCYBER/
[16] Cybersecurity and Infrastructure Security Agency - Wikipedia
[17] Cyber Crime — FBI

Federal Emergency Management Agency, U.S. (FEMA):

FEMA supports citizens and emergency personnel to prepare for, protect against, respond to, recover from, and mitigate all hazards, including cyber risks.[18] FEMA's mission is to reduce the loss of life and property and protect institutions from all hazards, including cyber risks.

Secret Service, U.S. (USSS)

The USSS's goal is to protect the nation's financial infrastructure and maintain a safe environment for the American people to conduct financial transactions. Its mission is to investigate complex cyber-enabled financial crimes.[19]

Industry and Non-Profit Partners

CyberHawaii

CyberHawaii is an information sharing and workforce development non-profit organization committed to developing and enhancing Hawai'i's cybersecurity capabilities. CyberHawaii is committed to a whole community approach that will help to mitigate cyber risks for all community members, develop educational and workforce pathways for students, augment cyber services being delivered by government agencies, commercial entities, research organizations and Community Based Organizations, and inform local decision makers about cyber security risks and solutions.

DRFortress

Based in Honolulu, DRFortress is the largest and the only carrier-neutral data center and cloud marketplace operating in Hawai'i. They support needs of Hawai'i's enterprises, content companies, system integrators, carriers, wireless service providers, cable companies and ISPs.[20]

Hawai'ian Electric Company

Hawai'ian Electric serves 95 percent of Hawai'i's 1.4 million residents on the islands of Oahu, Maui, Hawai'i, Lanai and Molokai.[21]

[18] FEMA Strategic Plan: 2022-2026 - Homeland Security Digital Library (hsdl.org)
[19] https://www.secretservice.gov/investigation/cyber
[20] https://www.drfortress.com/about/
[21] https://www.hawaiianelectric.com/about-us

Hawai‘i Gas

Since 1904, Hawai‘i Gas has been the only franchised gas utility in the State of Hawai‘i. They installed gas pipeline infrastructure, built bulk storage facilities with access to the harbor, and developed a highly skilled workforce on every major island. Gas energy is a critical part of the fuel mix in Hawai‘i.[22]

Hawai’ian Telecom

Hawai’ian Telcom provides integrated communications, including High-Speed Internet, data, video entertainment, and local and long-distance voice services in Hawai‘i.[23]

Kauai Island Utility Cooperative

Kauai Island Utility Cooperative was formed in November of 2002 and operates as a not-for-profit organization that is owned by its members and governed by an elected board of directors.[24]

Par Pacific

The Par owns the East refinery, located on the Hawai’ian Island of Oahu. The refinery, together with the logistics and retail arms of their Hawai‘i operations, provides fuels to a network throughout Hawai‘i, and distributes fuels via pipelines on Oahu and on barges to all major harbors in the state.[25]

The Queen's Health System

The Queen’s Health System is a nonprofit health care organization in Hawai‘i. With four hospitals and more than 70 preventive, specialty health care locations and labs, it is the state’s largest employer.

[22] https://www.hawaiigas.com/about-us
[23] https://www.hawaiiantel.com/aboutus
[24] https://www.kiuc.coop/about-us
[25] https://www.parpacific.com/operations/refining-logistics/hawaii

State Partners

Hawai‘i Department of the Attorney General

The Attorney General is the chief legal officer and chief law enforcement officer of the State of Hawai‘i. The Attorney General is appointed by the Governor. 180 attorneys and over 500 professional and support personnel assist the Attorney General in fulfilling the responsibilities of the office.

Hawai‘i State Department of Education (DOE)

The Hawai‘i State Department of Education (DOE) is the state-level agency responsible for overseeing the public education system in the state of Hawai‘i. It is the largest single state educational system in the United States. The HIDOE is responsible for managing and operating public schools in Hawai‘i, from kindergarten through grade 12, and it serves both students and educators across the state.[26]

Hawai‘i State Department of Health (DOH)

The Hawai‘i State Department of Health (DOH) is responsible for overseeing public health and environmental quality in the state of Hawai‘i. The Hawai‘i State Department of Health plays a vital role in safeguarding the health and well-being of the people of Hawai‘i by addressing a wide range of public health and environmental concerns. It works in collaboration with local communities, healthcare providers, and other stakeholders to fulfill its mission.[27]

Hawai‘i State Department of Human Services (DHS)

The Hawai‘i State Department of Human Services (DHS) is a state government agency responsible for providing a wide range of social services and assistance programs to the residents of Hawai‘i. Its primary mission is to promote the well-being and self-sufficiency of individuals and families in need by offering various support services and benefits.[28]

Hawai‘i State Department of Transportation (DOT)

The Hawai‘i Department of Transportation (DOT) is responsible for planning, designing, constructing, operating, and maintaining State facilities and infrastructures in all modes of

[26] https://www.hawaiipublicschools.org/Pages/Home.aspx
[27] https://health.hawaii.gov/about/office-of-the-director/
[28] https://humanservices.hawaii.gov/overview/

transportation (land, air, and water). To achieve these objectives, the Department coordinates with other State, County, Federal, and private agencies and programs.[29]

Hawai‘i Office of Homeland Security (OHS)

The Office of Homeland Security's (OHS) primary responsibility is to enhance Hawai‘i's security preparedness and resilience in an integrated, synergistic, relevant, proactive, flexible, cost effective, full-spectrum effort across all domains in order to prevent, protect, mitigate, respond to, and recover from attacks, natural disasters, and emerging threats. OHS also manages the Hawai‘i State Fusion Center (HSFC), a Hawai‘i State government program that facilitates intelligence sharing between local, state, and federal agencies, and the public and private sectors. OHS, in coordination with appropriate entities and individuals, develops, regularly updates, maintains, and exercises adaptable response plans to address cybersecurity risks, including significant cyber incidents as described in the Hawai‘i Cyber Disruption Response Plan.[30]

Hawai‘i Army National Guard (HING)

HING serves as the Senior Army National Guard command and control element in support of the JFHQ-State for Army units assigned to the State. HING provides trained, equipped, and ready forces capable of mobilizing in support of both Federal and State Missions.[31]

Hawai‘i Judiciary

The Judiciary is one of three branches of state government in Hawai‘i. The other two are the executive and legislative branches. As an independent government branch, the Judiciary is responsible for administering justice in an impartial, efficient, and accessible manner according to the law.[32]

Hawai‘i State Energy Office (HSEO)

The Hawai‘i State Energy Office (HSEO) is a government agency within the state of Hawai‘i that is dedicated to advancing the state's energy policy and sustainability goals. It operates under the Department of Business, Economic Development, and Tourism (DBEDT) and plays a central role in Hawai‘i's efforts to transition to a clean and sustainable energy future.

[29] https://hidot.hawaii.gov/about-us/
[30] https://dod.hawaii.gov/ohs/
[31] https://dod.hawaii.gov/hiarng/about/
[32] https://www.courts.state.hi.us/general_information/general_information

Hawai‘i State Legislature, House of Representatives and Senate

The Hawai‘i State Legislature is the legislative branch of the government of the state of Hawai‘i, responsible for making and passing laws for the state. It is a bicameral legislature, meaning it consists of two separate chambers: the Hawai‘i State House of Representatives and the Hawai‘i State Senate.[33]

Office of Enterprise Services (ETS)

ETS provides governance for executive branch IT projects and seeks to identify, prioritize and advance innovative initiatives with the greatest potential to increase efficiency, reduce waste, and improve transparency and accountability in state government. ETS also supports the management and operation of all state agencies by providing effective, efficient, coordinated and cost-beneficial computer and telecommunication services such that state program objectives may be achieved.[34]

Office of the Governor

The Hawai‘i Office of the Governor is the executive branch of the state government responsible for overseeing the administration of Hawai‘i and implementing state laws and policies. The Governor of Hawai‘i is the head of the executive branch and serves as the chief executive officer of the state. The Office of the Governor consists of the Governor, the Lieutenant Governor, and their respective staff.[35]

Office of Hawai’ian Affairs

OHA is a semi-autonomous state agency responsible for improving the wellbeing of all Native Hawai’ians through advocacy, research, community engagement, land management and the funding of community programs. The agency is governed by a Board of Trustees, made up of nine members who are elected statewide to serve four-year terms and set organizational policy. OHA is administered by a Chief Executive Officer, who is appointed by the Board of Trustees to oversee a staff of about 170 people.[36]

The HSEO focuses on various aspects of energy policy, conservation, renewable energy, and energy efficiency.[37]

[33] https://www.capitol.hawaii.gov/home.aspx
[34] https://ets.hawaii.gov/about/
[35] https://governor.hawaii.gov/
[36] https://www.oha.org/about/
[37] https://energy.hawaii.gov/who-we-are/

Local Partners

City and County of Honolulu

The City and County of Honolulu, a political and corporate body, consists of the island of Oahu, all other islands not included in any other county, adjacent waters, and is vested with all powers authorized by the State Constitution, the laws of the State of Hawai‘i, and the Revised Charter of the City and County of Honolulu. The City and County of Honolulu is the most densely populated of five counties within the state of Hawai‘i, with a population of approximately 905,601. It is organized as a mayor-council type of government in which there is a separation between legislative and executive functions. CSPC representatives from the City and County of Honolulu include the Honolulu Police Department and the Department of Information Technology.[38][39]

County of Hawai‘i

The County of Hawai‘i is coextensive of the Island of Hawai‘i and has an approximate population of 200,629. Hawai‘i County is the largest county in the state in terms of geography. CSPC representatives from the County of Hawai‘i include the Department of Information Technology.[40]

County of Kaua'i

The County of Kaua'i consists of the islands of Kaua‘i, Ni‘ihau, Lehua, and Ka‘ula. The approximate population is 73,298. CSPC representatives from the County of Kaua'i include the Information Technology Division and the Department of Water Supply.[41]

County of Maui

The County of Maui consists of the islands of Maui, Lana‘i, Moloka‘i (except for a portion of Moloka‘i that comprises Kalawao County), Kaho‘olawe, and Molokini. The approximate population is 164,754, CSPC representatives from the County of Maui include the Information Technology Services Division.[42]

[38] https://www.honolulu.gov/
[39] https://lrb.hawaii.gov/wp-content/uploads/CCHonolulu_guide.pdf
[40] https://www.hawaiicounty.gov/our-county
[41] https://www.kauai.gov/Home
[42] https://www.mauicounty.gov/

Higher Education Partners

University of Hawai‘i (UH)

As the state’s public system of higher education, the University of Hawai‘i System includes 3 universities, 7 community colleges and community-based learning centers across Hawai‘i. UH is the only provider of public higher education and also owns an employment training center, three university centers, four education centers, and various other research facilities distributed across six islands throughout the state of Hawai‘i.[43]

[43] https://www.hawaii.edu/about-uh/