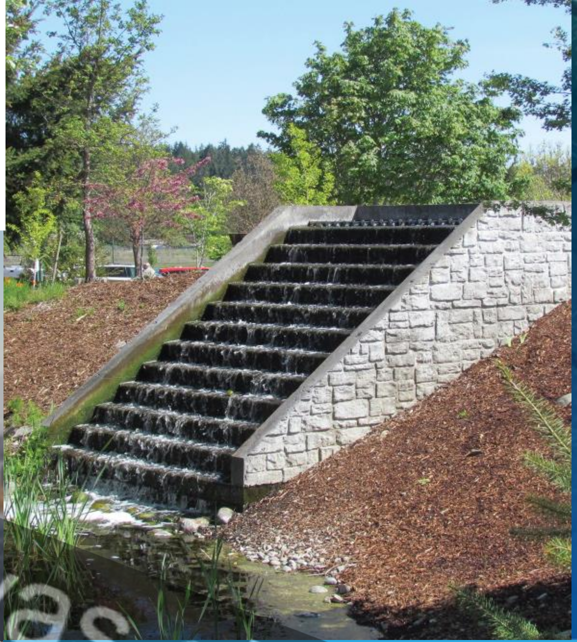


Ralph Ley

Workforce Development
Program Office

National & Homeland Security,

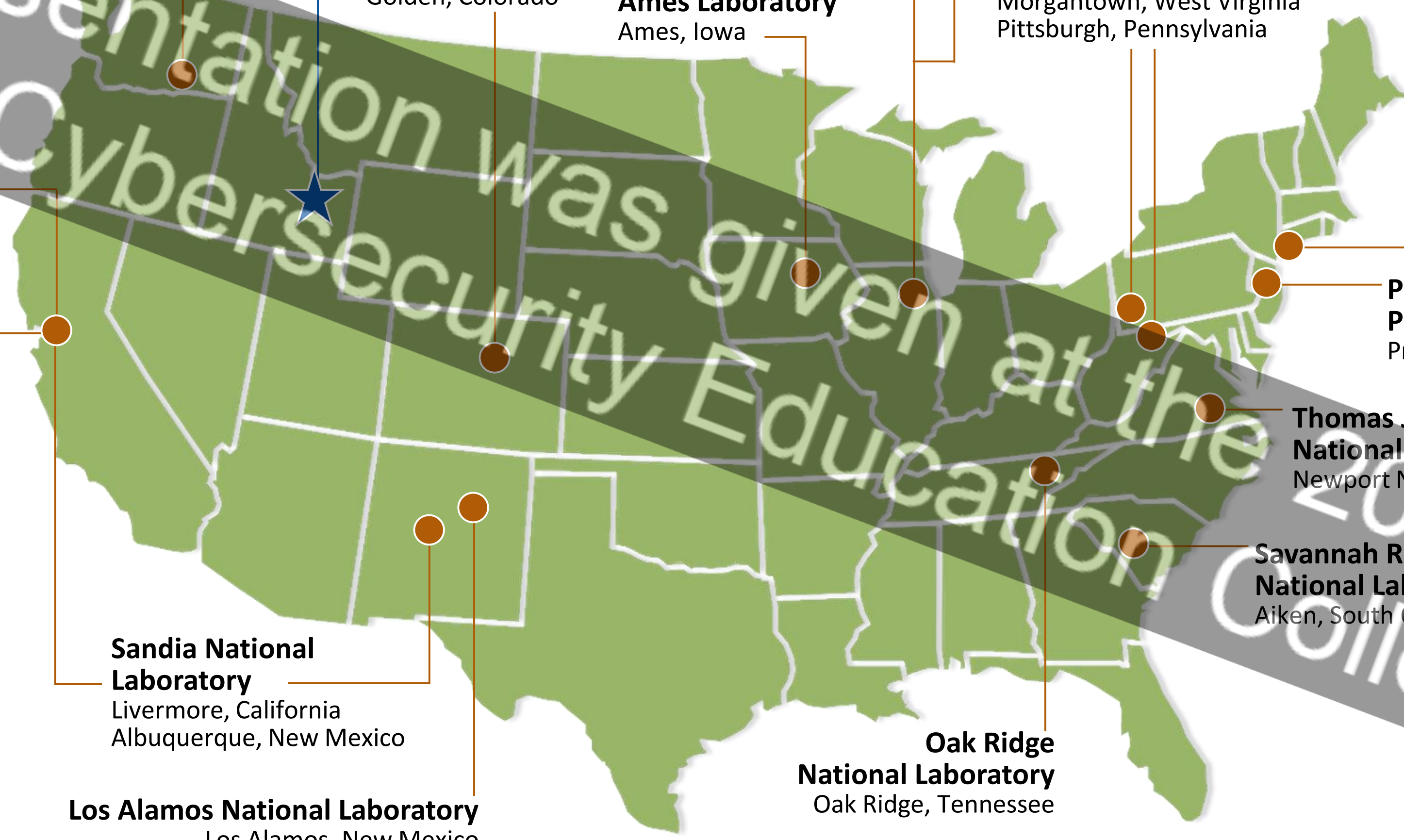
Idaho National Laboratory

Foundational Cyber Workforce Development and Education Requirements Analysis

INL is managed by Battelle Energy Alliance
for the US Department of Energy

Idaho National Laboratory

U.S. Department of Energy National Laboratories



Idaho National Laboratory
Idaho falls, Idaho

Pacific Northwest National Laboratory
Richland, Washington

National Renewable Energy Laboratory
Golden, Colorado

Argonne National Laboratory
Argonne, Illinois

Fermi National Accelerator Laboratory
Batavia, Illinois

Ames Laboratory
Ames, Iowa

National Energy Technology Laboratory
Morgantown, West Virginia
Pittsburgh, Pennsylvania

Brookhaven National Laboratory
Upton, New York

SLAC National Accelerator Laboratory
Menlo Park, California

Lawrence Berkeley National Laboratory
Berkeley, California

Lawrence Livermore National Laboratory
Livermore, California

Princeton Plasma Physics Laboratory
Princeton, New Jersey

Thomas Jefferson National Accelerator Facility
Newport News, Virginia

Savannah River National Laboratory
Aiken, South Carolina

Sandia National Laboratory
Livermore, California
Albuquerque, New Mexico

Los Alamos National Laboratory
Los Alamos, New Mexico

Oak Ridge National Laboratory
Oak Ridge, Tennessee

National and Homeland Security Mission Focus Areas

Industrial Control Systems Security

Secure and Resilient Grid

Wireless Security

Infrastructure & Risk Analysis

First Responder Training

Nuclear Safety and Security

Defense Systems

Solving security challenges in critical infrastructure protection and resiliency, nuclear and radiological security, and national defense.

Mission: Industrial Control System Security

Integrating Government, Academia, & Industry

Integrating Analysts, Engineers, & Computer Scientists

Threat, Vulnerability, & Consequence Analysis

Design and Engineering Culture Change

Workforce, Training Development and Delivery

Innovating and applying control-system cybersecurity solutions

INL National & Homeland Security Directorate Workforce Development Program Office

Address the most critical control systems and cybersecurity challenges that require a national collaborative, inter-disciplinary environment

Drive a culture change in engineering

Increase cybersecurity of systems deployed and under development

Enhanced partnerships

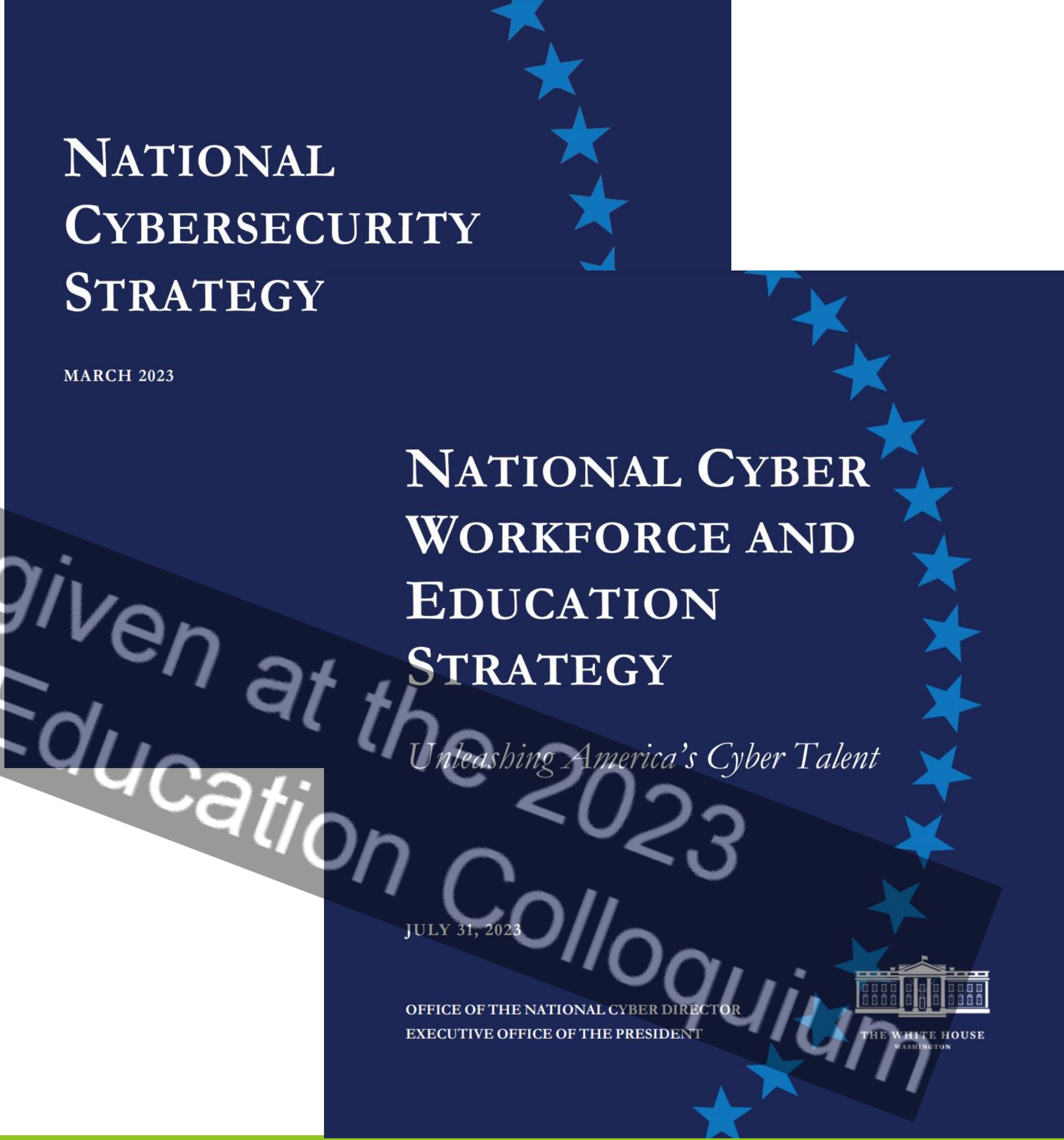
Advance control systems cybersecurity gaps

Accelerate workforce development

Support demand for control system cybersecurity talent

National Imperative – Defend Critical Infrastructure

- Expanding the use of minimum cybersecurity requirements in critical sectors
- Enabling public-private collaboration at the speed and scale necessary to defend critical infrastructure and essential services
- Defending and modernizing Federal networks and updating Federal incident response policy



NATIONAL CYBERSECURITY STRATEGY

MARCH 2023

NATIONAL CYBER WORKFORCE AND EDUCATION STRATEGY

Unleashing America's Cyber Talent

JULY 31, 2023

OFFICE OF THE NATIONAL CYBER DIRECTOR
EXECUTIVE OFFICE OF THE PRESIDENT

THE WHITE HOUSE
WASHINGTON

Accelerating Cyber Workforce Development

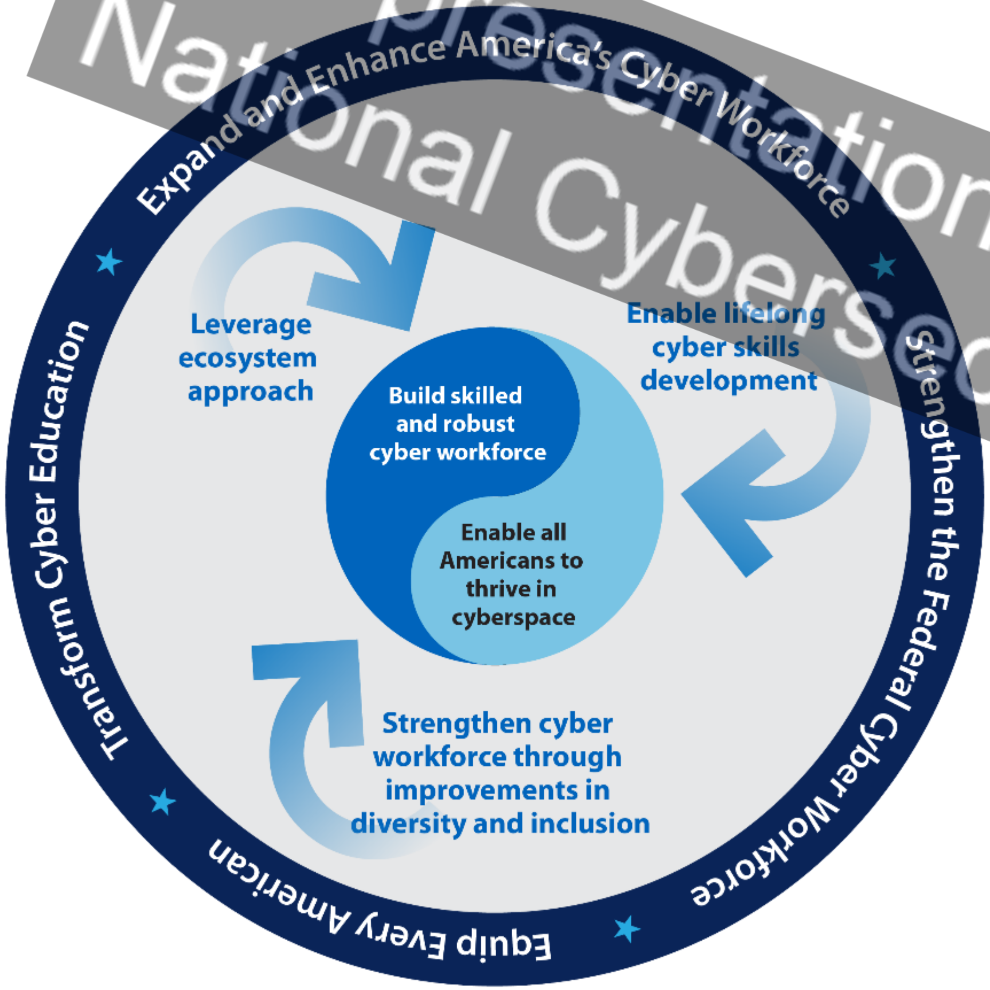
The National & Homeland Security Directorate at Idaho National Laboratory is creating models & pilots to address national workforce development needs

https://inl.gov/national-security-training/

Advancing our talent pipeline thru core R&D partnerships and educational opportunities

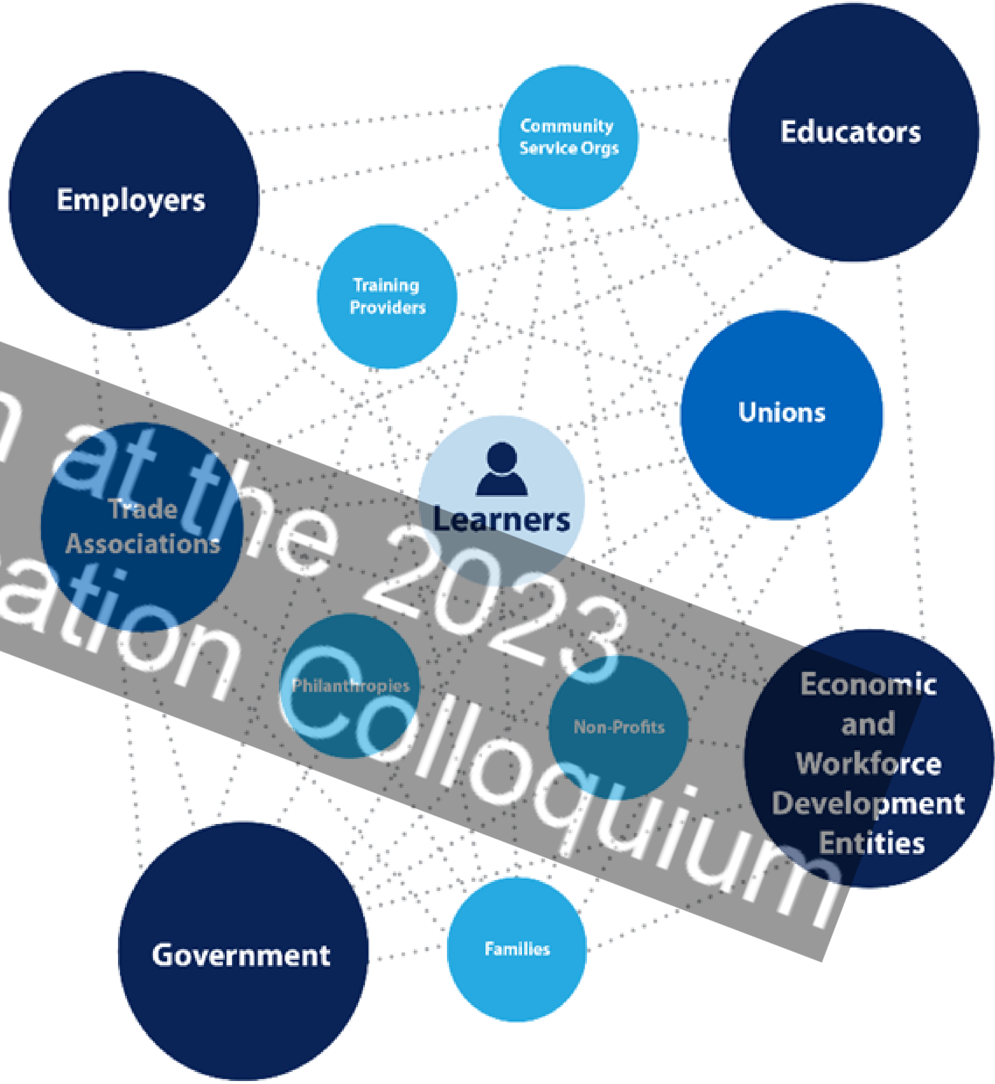
- CISA Training/Curriculum Sharing
- ICS Community of Practice
- Cyber CHAMP
- OT Defender Fellowship
- Consequence-driven Cyber-informed Engineering and Cyber Informed Engineering
- Cybercore Integration Center Academic Collaboration Laboratory
- Internships, Apprenticeships, Fellowships & Joint Appointments
- STEM Education & Outreach – Shareable Learning Modules

Adapting an Ecosystem Approach

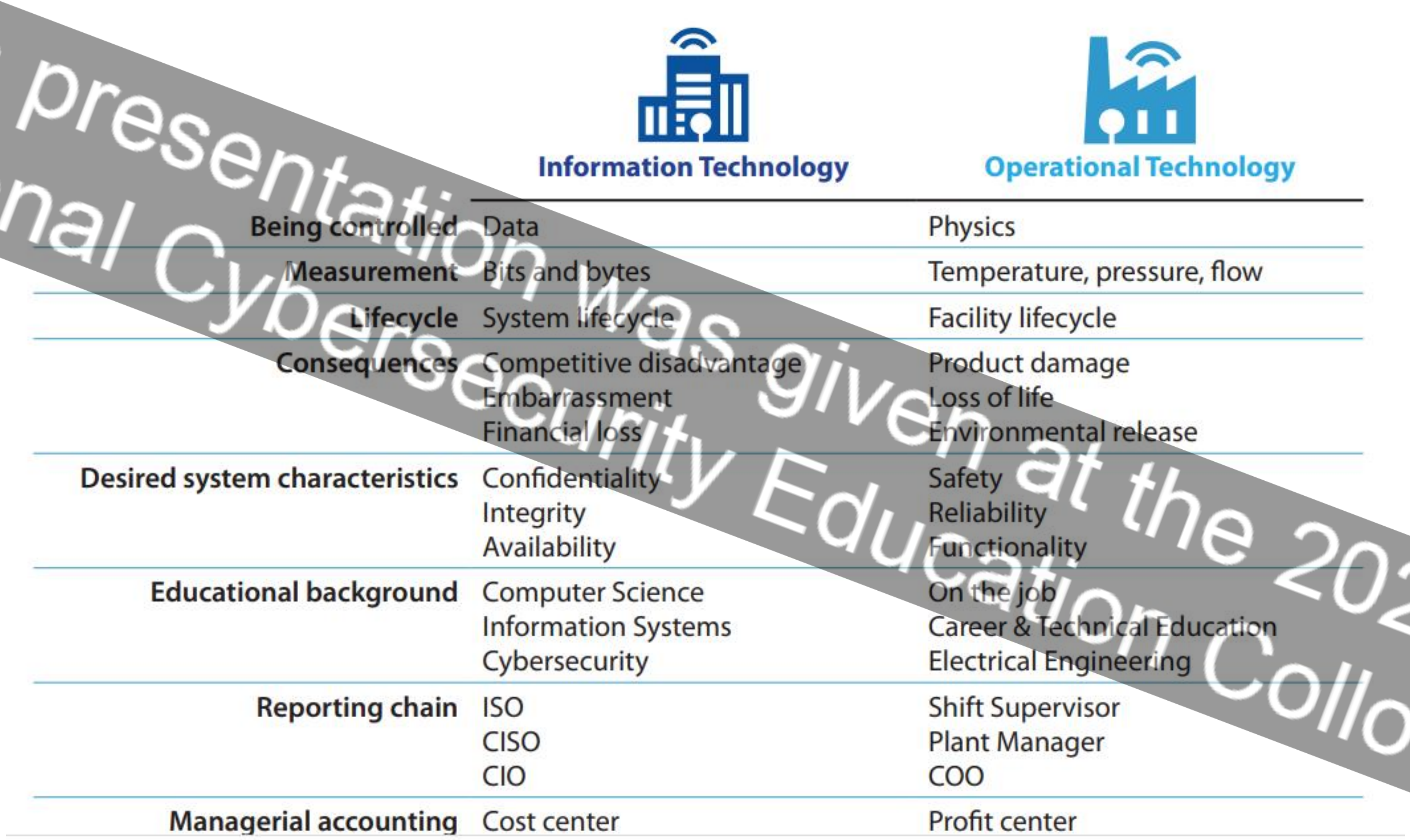

Expand and Enhance America's Cyber Workforce
Strengthen the Federal Cyber Workforce
Equip Every American
Transform Cyber Education
Leverage ecosystem approach
Enable lifelong cyber skills development
Strengthen cyber workforce through improvements in diversity and inclusion
Build skilled and robust cyber workforce
Enable all Americans to thrive in cyberspace

Cyber Education and Workforce Development Ecosystems

- Stakeholders may include: learners (students, job seekers, and employees), employers, educators, trainers, government at all levels, trade associations, unions, economic and workforce development entities; non-profit organizations, civil society organizations, philanthropies
- Ecosystems take diverse forms; must be suited to specific local, regional, functional needs



Information Technology (IT) and Operational Technology (OT)



	Information Technology	Operational Technology
Being controlled	Data	Physics
Measurement	Bits and bytes	Temperature, pressure, flow
Lifecycle	System lifecycle	Facility lifecycle
Consequences	Competitive disadvantage Embarrassment Financial loss	Product damage Loss of life Environmental release
Desired system characteristics	Confidentiality Integrity Availability	Safety Reliability Functionality
Educational background	Computer Science Information Systems Cybersecurity	On the job Career & Technical Education Electrical Engineering
Reporting chain	ISO CISO CIO	Shift Supervisor Plant Manager COO
Managerial accounting	Cost center	Profit center

Understanding the Cyber Workforce Development Gap

Asked by DHS in 2018 to research cyber workforce development issues. As such, INL has:

- Created an Industrial Cyber Community of Practice in 2020
- Conducted 5 years of foundational research
- Performed workforce development evaluations across industries, sectors and regions

Major discovery: **This is not a cyber issue, this is a business strategy issue**

INL's Research Response ~ The creation of a process, framework, and tool that can:

Step 1

Assess cyber "health" and "maturity"

Step 2

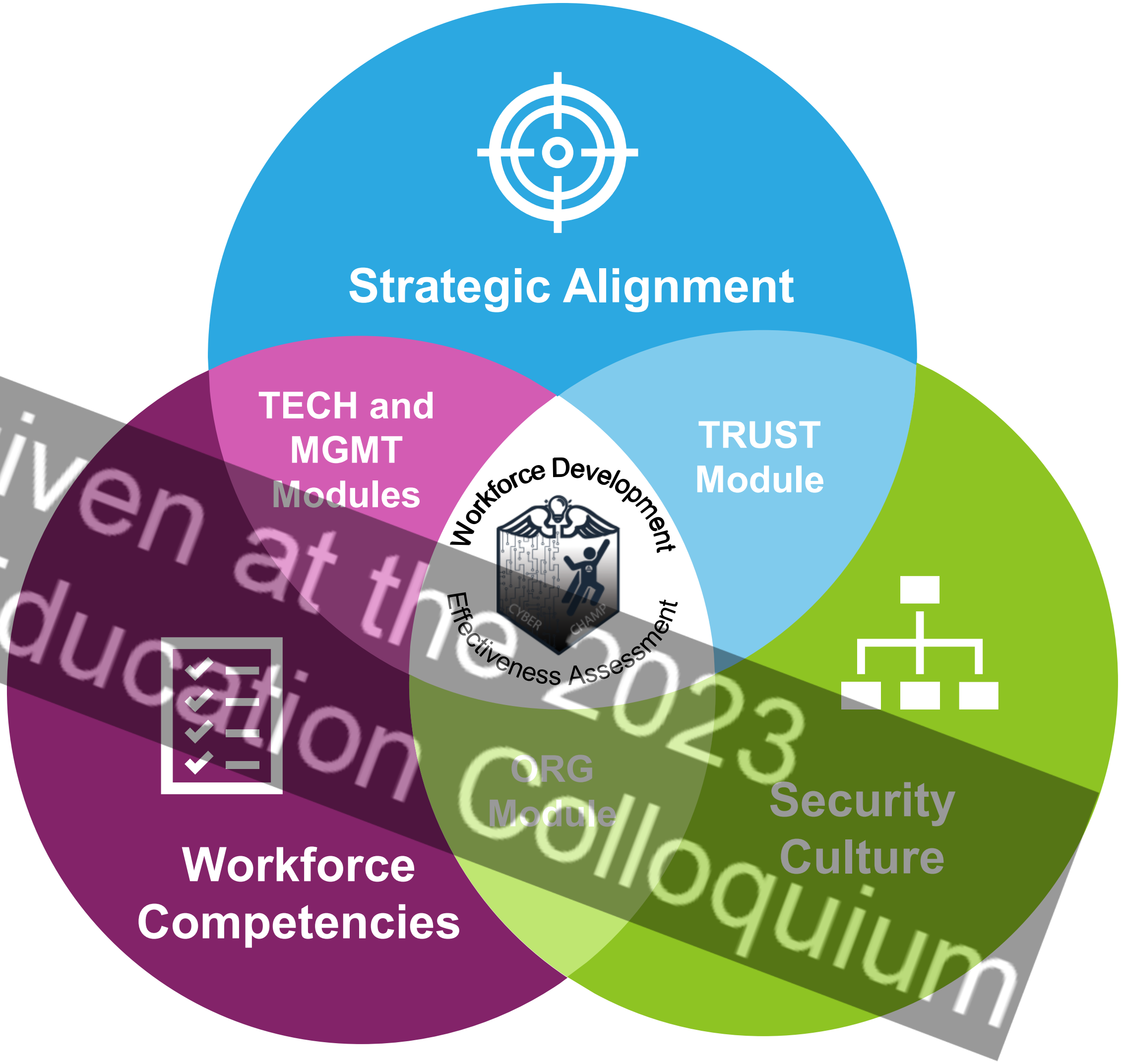
Identify most effective organizational cyber structure

Step 3

Determine competency-based training needs and recommendations

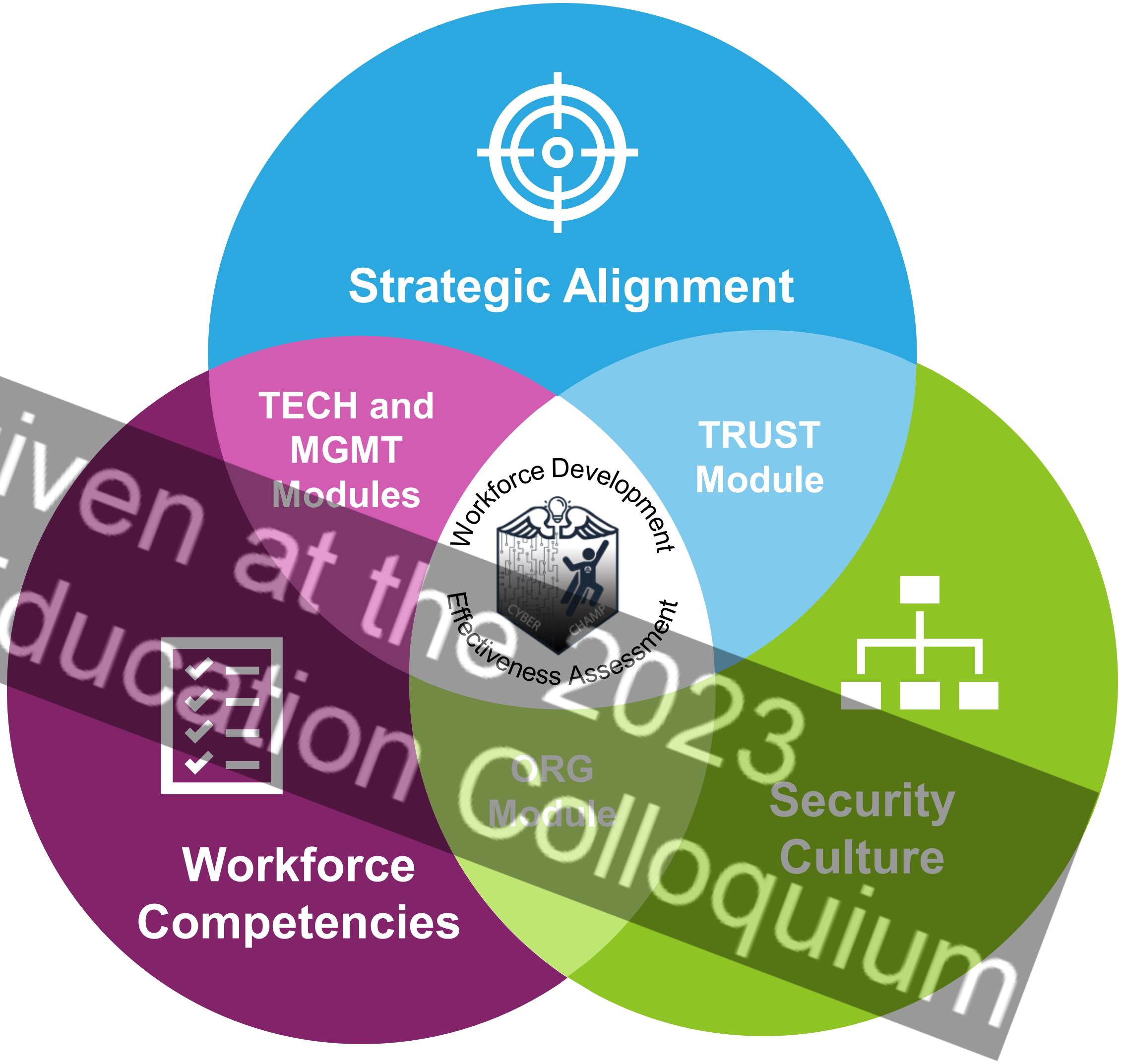
Cyber Competency Health and Maturity Progression Model (Cyber-CHAMP©) Introduction

- A business tool to assess organizational needs from a cyber workforce development perspective.
- Built from national / international standards and frameworks.
- Built with industry collaboration, feedback, years of research, and industry evaluations across multiple sectors.
- Approach is tailored and results are unique to each organization’s workforce profile.



Cyber Competency Health and Maturity Progression Model (Cyber-CHAMP©) Future

- Develop cybersecurity workforce trends by sector
- Determine what curriculum needs to be developed of local businesses and municipalities
- Create cyber risk dashboards and meet with insurance companies to identify ROI



Job Title Discrepancy from Org Profile/Tech Modules

Job Title Sources	Individual 1
Employee Listed Title	Cybersecurity Technical Analyst / Penetration Tester
Org Chart Title	Vulnerability Assessments
HR Title	Cybersecurity Technical Analyst

Job Title Sources	Individual 2
Employee Listed Title	ICS Cyber Architect: ALT ISSM
Org Chart Title	Sys Admin, Strategy and Data Architect (Strictly ICS System)
HR Title	Cybersecurity Analyst

Job Title Sources	Individual 3
Employee Listed Title	Information System Security Manager (ISSM)
Org Chart Title	Unclassified Cybersecurity Policy Manager
HR Title	Business Services Supervisor

Job Title Sources	Individual 4
Employee Listed Title	Information System Security Engineer (ISSE)
Org Chart Title	Classified Cybersecurity Analyst
HR Title	Cybersecurity Technical Analyst

Analysis: Org. Profile/Tech Module

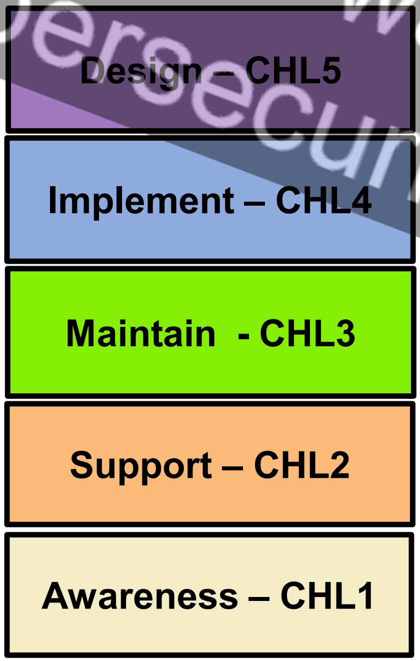
Technical analysis

Result: Workforce development and training roadmaps for individuals

All tasks mapped to a competency level

- Each individual chooses tasks they perform.
- All tasks are mapped to a competency level.
- All tasks are mapped to learning objectives in course offerings.

Cyber-CHAMP Competencies



Design – CHL5

Implement – CHL4

Maintain - CHL3

Support – CHL2

Awareness – CHL1

Chosen tasks mapped to competencies

Job Task Analysis Competency Alignment

Primary

- Maintain: 45.24%

Secondary

- Implementation: 23.81%

Tertiary

- Awareness: 14.29%

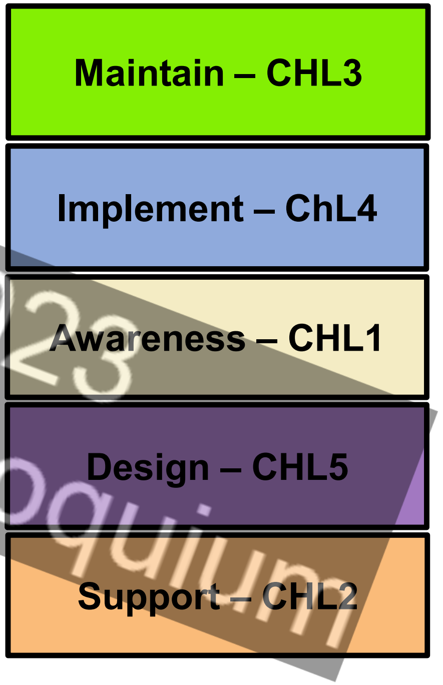
Quartern

- Design: 11.90%

Fifth Order

- Support: 4.76%

Competencies by Tasking



Maintain – CHL3

Implement – ChL4

Awareness – CHL1

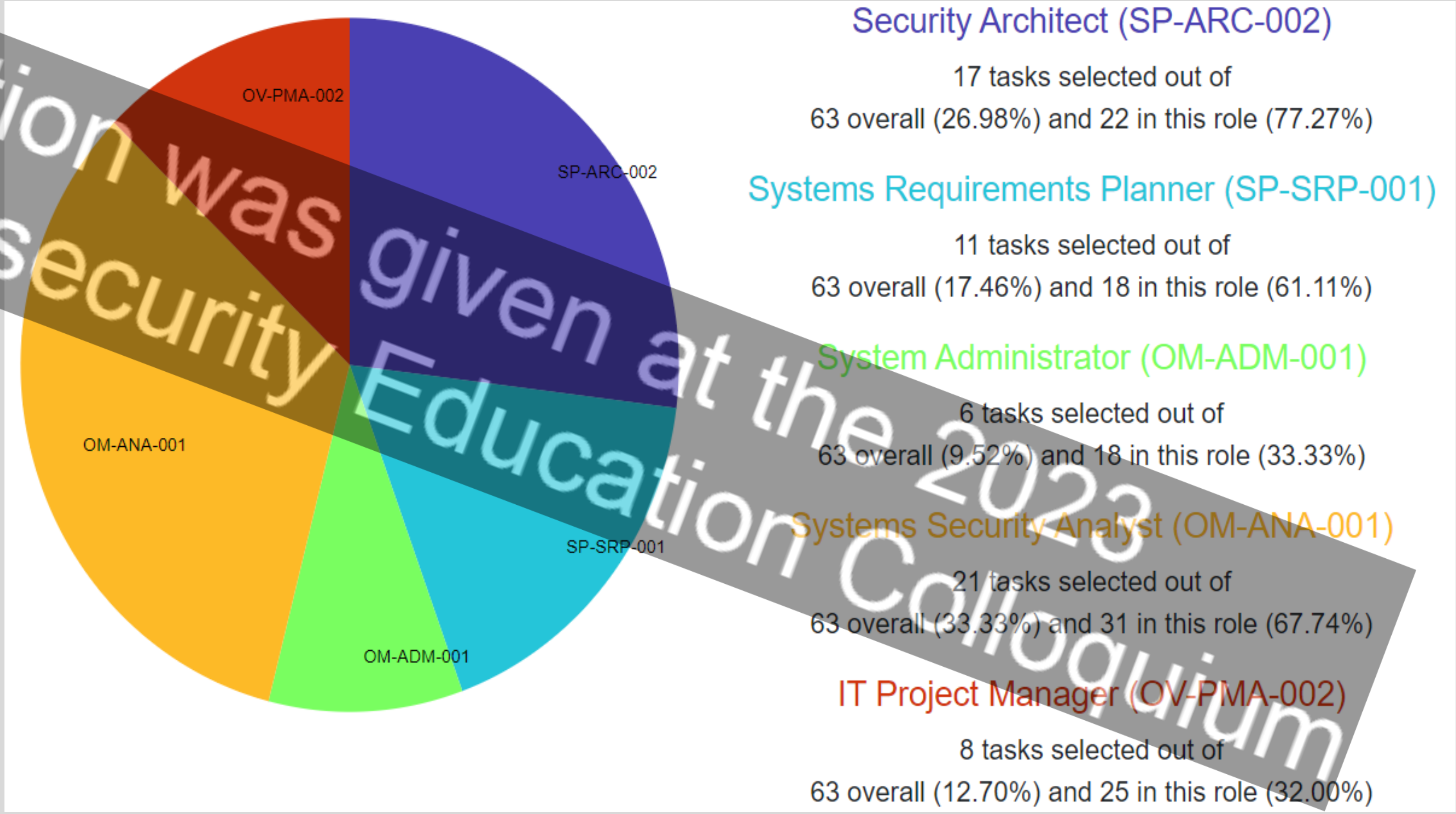
Design – CHL5

Support – CHL2

Technical Job Role Analysis

Result: Job decomposition intro roles by tasking or responsibility/duties

- Is this the work this person should be doing?
- What things are they doing that are not part of their primary tasking?
- How can I hire someone to do the same job as this individual?
- What education and training does this individual need to become and remain competent?



Security Architect (SP-ARC-002)

17 tasks selected out of
63 overall (26.98%) and 22 in this role (77.27%)

Systems Requirements Planner (SP-SRP-001)

11 tasks selected out of
63 overall (17.46%) and 18 in this role (61.11%)

System Administrator (OM-ADM-001)

6 tasks selected out of
63 overall (9.52%) and 18 in this role (33.33%)

Systems Security Analyst (OM-ANA-001)

21 tasks selected out of
63 overall (33.33%) and 31 in this role (67.74%)

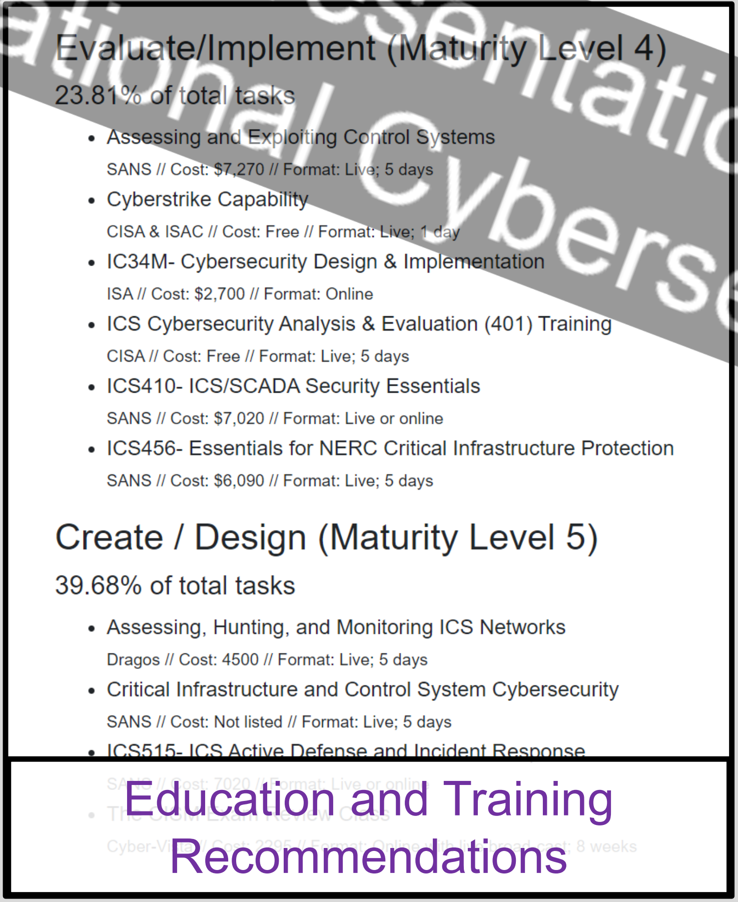
IT Project Manager (OV-PMA-002)

8 tasks selected out of
63 overall (12.70%) and 25 in this role (32.00%)

Technical Competency Take-Aways

Result: Education, Training, and Certification Recommendations

Mapping to industry training



Evaluate/Implement (Maturity Level 4)

23.81% of total tasks

- Assessing and Exploiting Control Systems

  SANS // Cost: $7,270 // Format: Live; 5 days
- Cyberstrike Capability

  CISA & ISAC // Cost: Free // Format: Live; 1 day
- IC34M- Cybersecurity Design & Implementation

  ISA // Cost: $2,700 // Format: Online
- ICS Cybersecurity Analysis & Evaluation (401) Training

  CISA // Cost: Free // Format: Live; 5 days
- ICS410- ICS/SCADA Security Essentials

  SANS // Cost: $7,020 // Format: Live or online
- ICS456- Essentials for NERC Critical Infrastructure Protection

  SANS // Cost: $6,090 // Format: Live; 5 days

Create / Design (Maturity Level 5)

39.68% of total tasks

- Assessing, Hunting, and Monitoring ICS Networks

  Dragos // Cost: 4500 // Format: Live; 5 days
- Critical Infrastructure and Control System Cybersecurity

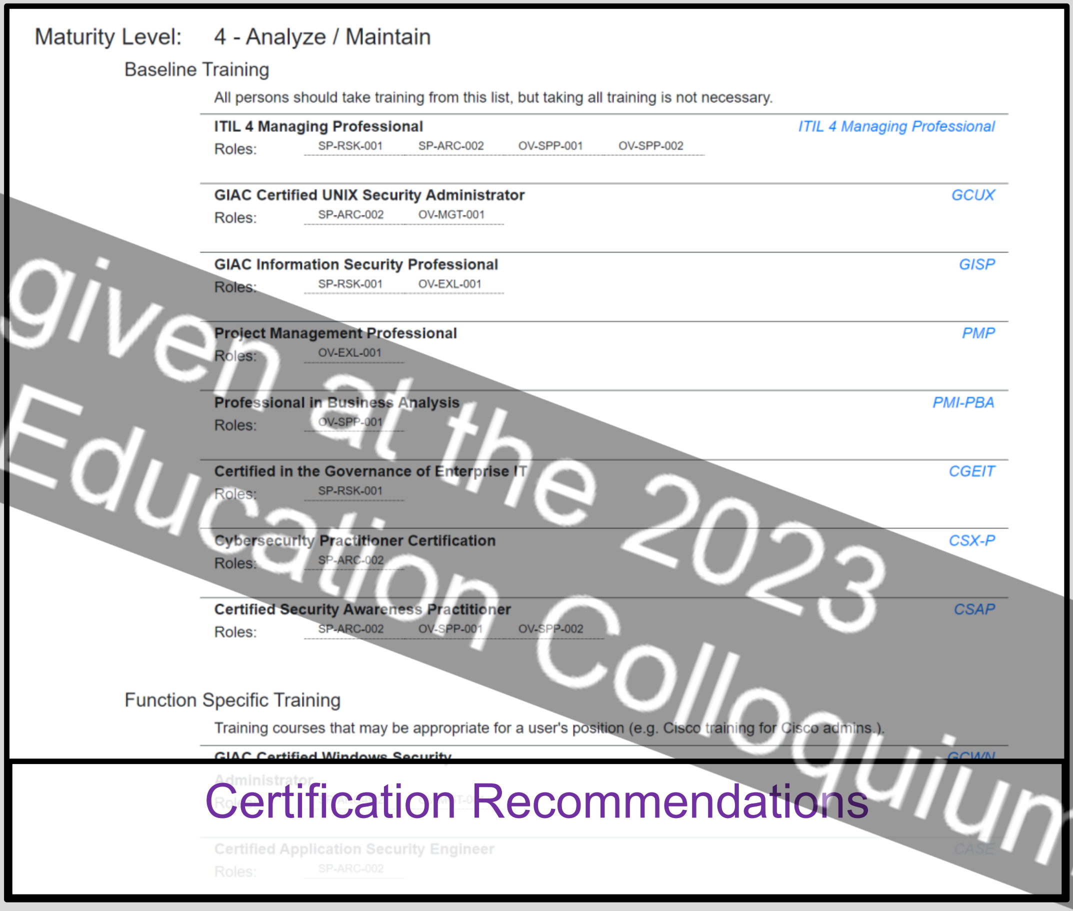
  SANS // Cost: Not listed // Format: Live; 5 days
- ICS515- ICS Active Defense and Incident Response

  SANS // Cost: 7020 // Format: Live or online
- The CISM Exam Review Class

  Cyber-Vista // Cost: 2295 // Format: Online with live broad-cast; 8 weeks

Education and Training Recommendations

Mapping to industry certifications



Maturity Level: 4 - Analyze / Maintain

Baseline Training

All persons should take training from this list, but taking all training is not necessary.

ITIL 4 Managing Professional *ITIL 4 Managing Professional*
Roles: SP-RSK-001 SP-ARC-002 OV-SPP-001 OV-SPP-002

GIAC Certified UNIX Security Administrator *GCUX*
Roles: SP-ARC-002 OV-MGT-001

GIAC Information Security Professional *GISP*
Roles: SP-RSK-001 OV-EXL-001

Project Management Professional *PMP*
Roles: OV-EXL-001

Professional in Business Analysis *PMI-PBA*
Roles: OV-SPP-001

Certified in the Governance of Enterprise IT *CGEIT*
Roles: SP-RSK-001

Cybersecurity Practitioner Certification *CSX-P*
Roles: SP-ARC-002

Certified Security Awareness Practitioner *CSAP*
Roles: SP-ARC-002 OV-SPP-001 OV-SPP-002

Function Specific Training

Training courses that may be appropriate for a user's position (e.g. Cisco training for Cisco admins.).

GIAC Certified Windows Security Administrator *GCWN*
Roles: [illegible]

Certified Application Security Engineer *CASE*
Roles: SP-ARC-002

Certification Recommendations

TECH Module Deliverables and Benefits

Deliverable	Benefit
Individualized competency level mapping based on tasking	Targeted competency roadmap for each individual. More efficient use of organizational resources spent.
Task-based competency decomposition for each individual's position	Technical personnel job role and tasking transparency. Organization has clarity of each individual's technical roles and tasks to provide insight into proper tasking alignment.
Tailored education and training recommendations	Each individual becomes and remains competent. More efficient use of organizational resources spent.
Customized certification recommendations	Provides individuals with suggestions to achieve a higher technical competency.

Management analysis

Result: Workforce development and training roadmaps for individuals

All skills mapped to a competency level

- Each individual chooses skills they perform.
- All skills are mapped to a competency level.
- All skills are mapped to learning objectives in course offerings.

Cyber-CHAMP Competencies

Strategy – CHL5

Policy– CHL4

Direction - CHL3

Process– CHL2

Execution – CHL1

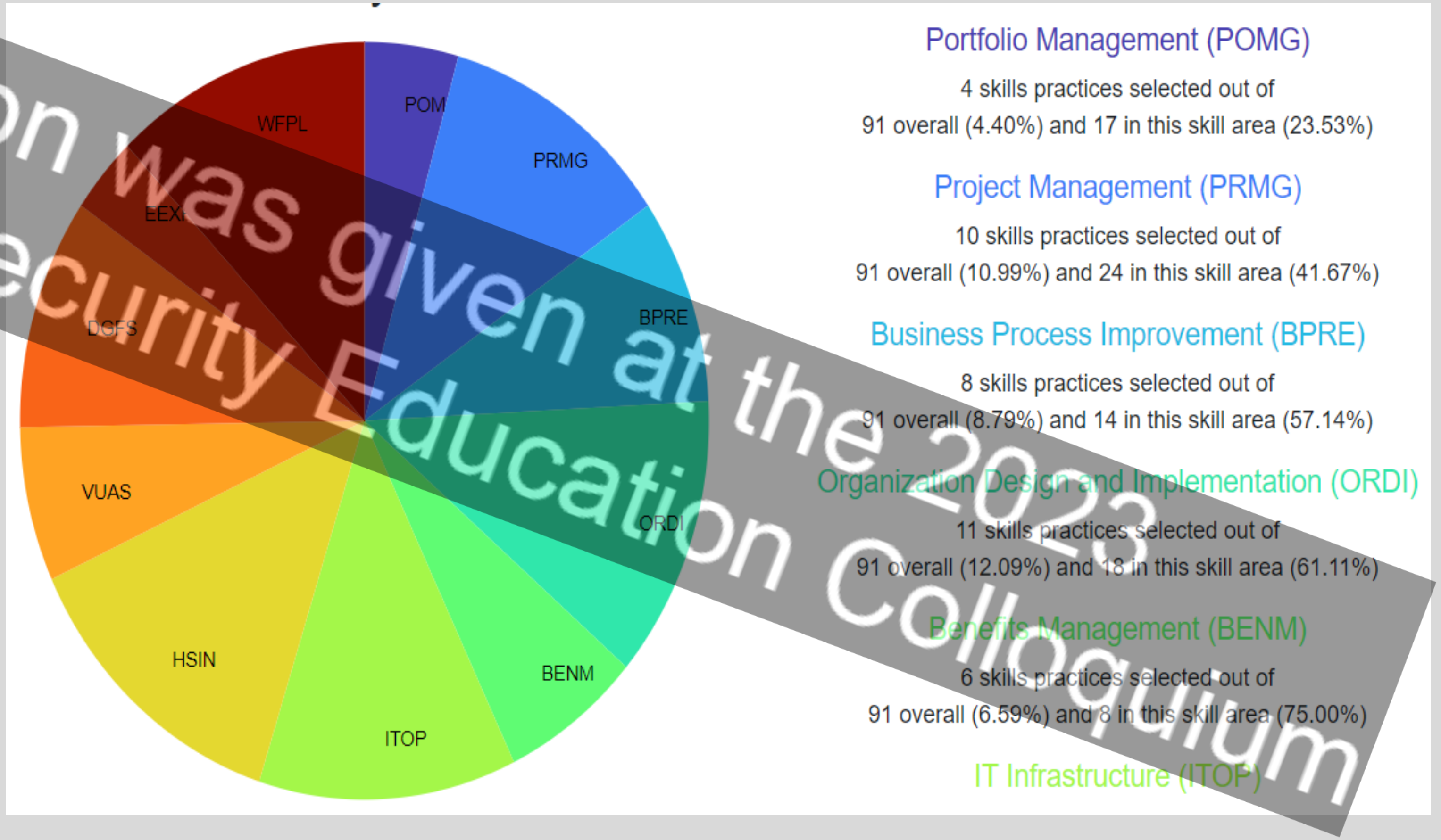
Chosen skills mapped to competencies

Job Skill Analysis Competency Alignment	Competencies by Skill
Form Policy: 60.44%	Policy– CHL4
Provide Direction: 12.09%	Direction - CHL3
Build Process/Procedure: 9.89%	Process– CHL2
Execution: 8.79%	Execution – CHL1
Establish Strategy: 8.79%	Strategy – CHL5

Management Job Role Analysis

Result: Job decomposition intro roles by tasking or responsibility/duties

- Are cyber skills acceptable at this level of management?
- What cyber management skills should this individual pursue?
- How can I hire someone to do the same job as this individual?
- What education/training does this manager need to become cyber cognizant and competent?



Portfolio Management (POMG)

4 skills practices selected out of
91 overall (4.40%) and 17 in this skill area (23.53%)

Project Management (PRMG)

10 skills practices selected out of
91 overall (10.99%) and 24 in this skill area (41.67%)

Business Process Improvement (BPRE)

8 skills practices selected out of
91 overall (8.79%) and 14 in this skill area (57.14%)

Organization Design and Implementation (ORDI)

11 skills practices selected out of
91 overall (12.09%) and 18 in this skill area (61.11%)

Benefits Management (BENM)

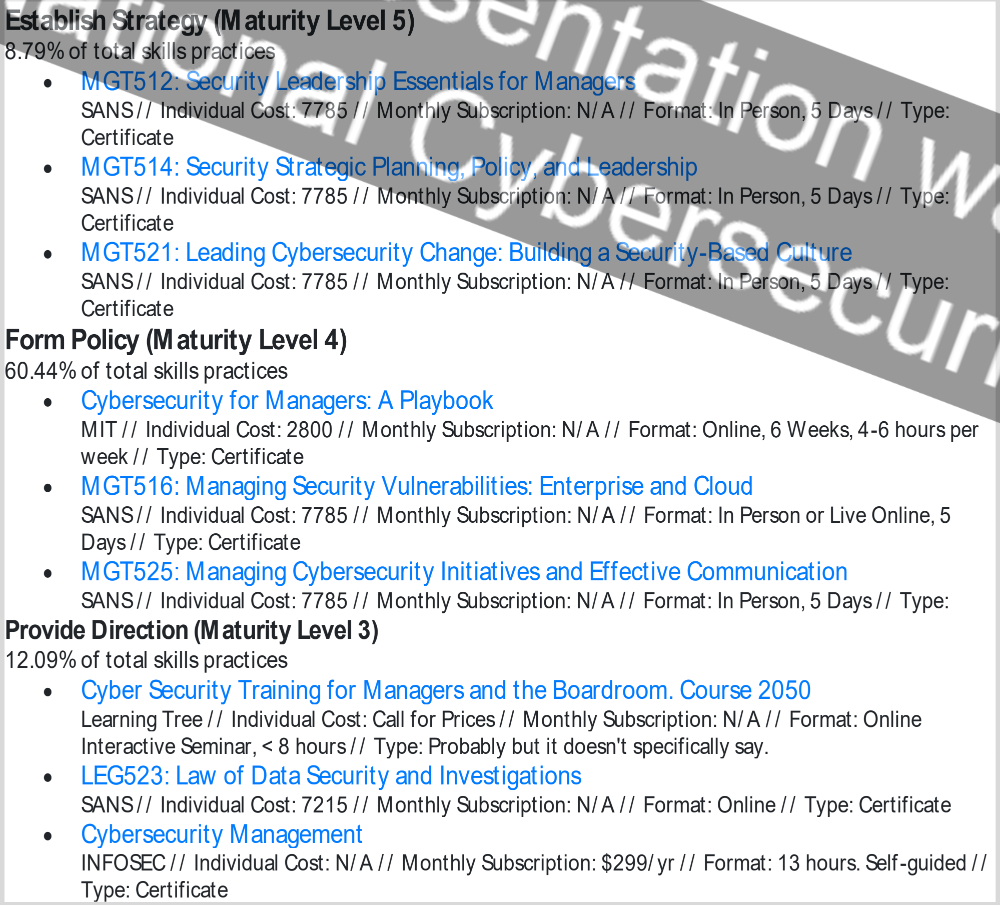
6 skills practices selected out of
91 overall (6.59%) and 8 in this skill area (75.00%)

IT Infrastructure (ITOP)

Management Competency Take-Aways

Result: Education, Training, and Certification Recommendations

Mapping to industry training



Establish Strategy (Maturity Level 5)

8.79% of total skills practices

- MGT512: Security Leadership Essentials for Managers
  SANS // Individual Cost: 7785 // Monthly Subscription: N/A // Format: In Person, 5 Days // Type: Certificate
- MGT514: Security Strategic Planning, Policy, and Leadership
  SANS // Individual Cost: 7785 // Monthly Subscription: N/A // Format: In Person, 5 Days // Type: Certificate
- MGT521: Leading Cybersecurity Change: Building a Security-Based Culture
  SANS // Individual Cost: 7785 // Monthly Subscription: N/A // Format: In Person, 5 Days // Type: Certificate

Form Policy (Maturity Level 4)

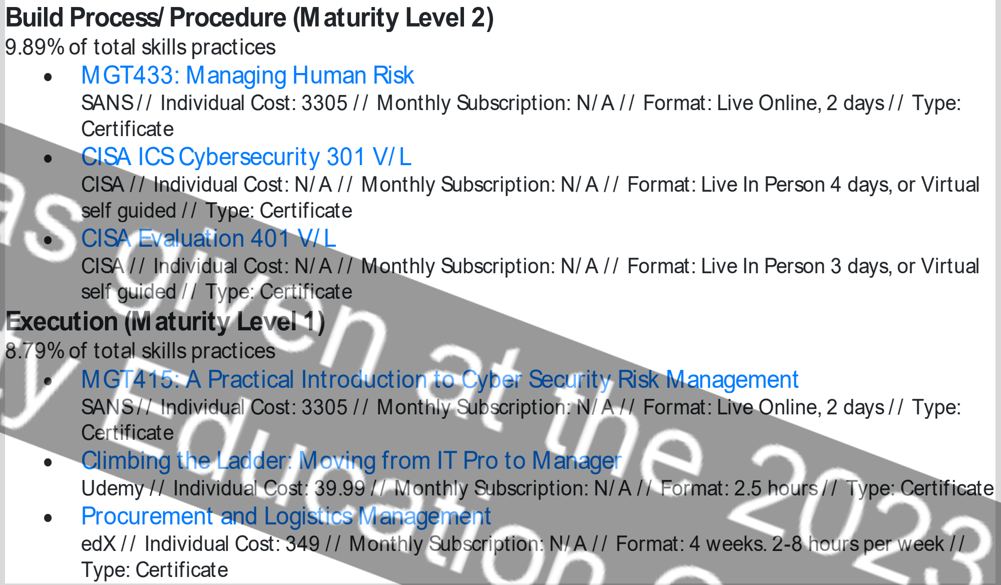
60.44% of total skills practices

- Cybersecurity for Managers: A Playbook
  MIT // Individual Cost: 2800 // Monthly Subscription: N/A // Format: Online, 6 Weeks, 4-6 hours per week // Type: Certificate
- MGT516: Managing Security Vulnerabilities: Enterprise and Cloud
  SANS // Individual Cost: 7785 // Monthly Subscription: N/A // Format: In Person or Live Online, 5 Days // Type: Certificate
- MGT525: Managing Cybersecurity Initiatives and Effective Communication
  SANS // Individual Cost: 7785 // Monthly Subscription: N/A // Format: In Person, 5 Days // Type:

Provide Direction (Maturity Level 3)

12.09% of total skills practices

- Cyber Security Training for Managers and the Boardroom. Course 2050
  Learning Tree // Individual Cost: Call for Prices // Monthly Subscription: N/A // Format: Online Interactive Seminar, < 8 hours // Type: Probably but it doesn't specifically say.
- LEG523: Law of Data Security and Investigations
  SANS // Individual Cost: 7215 // Monthly Subscription: N/A // Format: Online // Type: Certificate
- Cybersecurity Management
  INFOSEC // Individual Cost: N/A // Monthly Subscription: $299/yr // Format: 13 hours. Self-guided // Type: Certificate



Build Process/Procedure (Maturity Level 2)

9.89% of total skills practices

- MGT433: Managing Human Risk
  SANS // Individual Cost: 3305 // Monthly Subscription: N/A // Format: Live Online, 2 days // Type: Certificate
- CISA ICS Cybersecurity 301 V/L
  CISA // Individual Cost: N/A // Monthly Subscription: N/A // Format: Live In Person 4 days, or Virtual self guided // Type: Certificate
- CISA Evaluation 401 V/L
  CISA // Individual Cost: N/A // Monthly Subscription: N/A // Format: Live In Person 3 days, or Virtual self guided // Type: Certificate

Execution (Maturity Level 1)

8.79% of total skills practices

- MGT415: A Practical Introduction to Cyber Security Risk Management
  SANS // Individual Cost: 3305 // Monthly Subscription: N/A // Format: Live Online, 2 days // Type: Certificate
- Climbing the Ladder: Moving from IT Pro to Manager
  Udemy // Individual Cost: 39.99 // Monthly Subscription: N/A // Format: 2.5 hours // Type: Certificate
- Procurement and Logistics Management
  edX // Individual Cost: 349 // Monthly Subscription: N/A // Format: 4 weeks. 2-8 hours per week // Type: Certificate

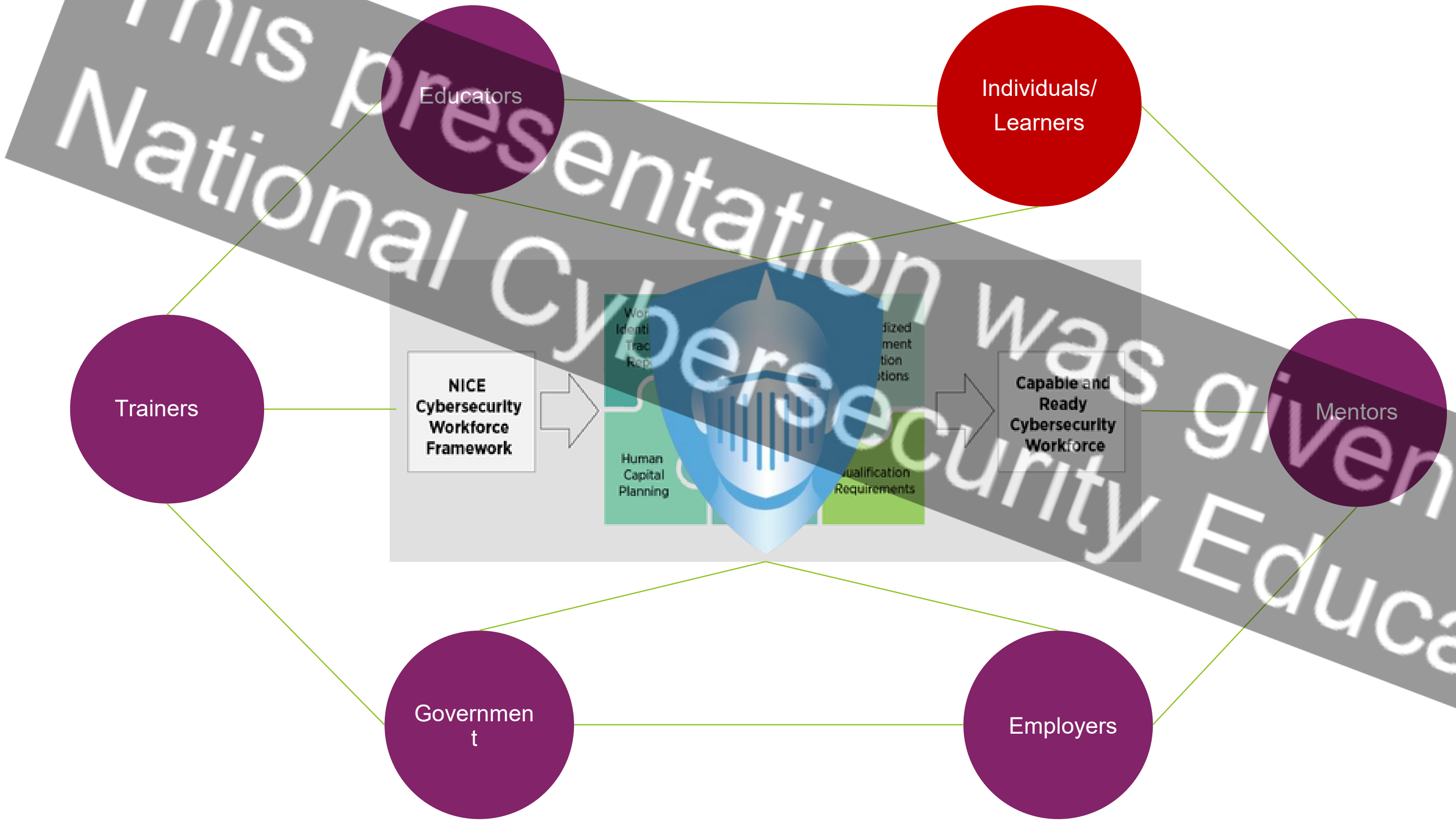
MGMT Module Deliverables and Benefits

Deliverable	Benefit
Individualized competency level mapping based on skills	Targeted competency roadmap for each individual. More efficient use of organizational resources spent.
Responsibility/duty-based competency decomposition for each individual's position	Management personnel job role and skill transparency. Organization management roles and skills clarity to provide insight into proper cybersecurity education and training.
Tailored education and training recommendations	Each individual becomes and remains competent. More efficient use of organizational resources spent.
Management security program roles and responsibilities analysis	Increased awareness and understanding for management roles and responsibilities towards establishing and maintaining a security program

Cyber-CHAMP© Summary

- Incorporates cyber into the business strategy
- Organizational view of their workforce's cyber educational needs
  - Employees and Managers
  - Actionable recommendations for improvement
- Provides the foundation for establishing an understanding of cyber as it relates to risk
  - Valid for multiple infrastructure sectors and organizations
- Scalable to any size of organization
- Results are directly applicable to enhancing the academic approach
  - Adjust curricula
  - Create and apply apprenticeships

CyberKnights – Collaborative Framework



Ways to use CyberKnights

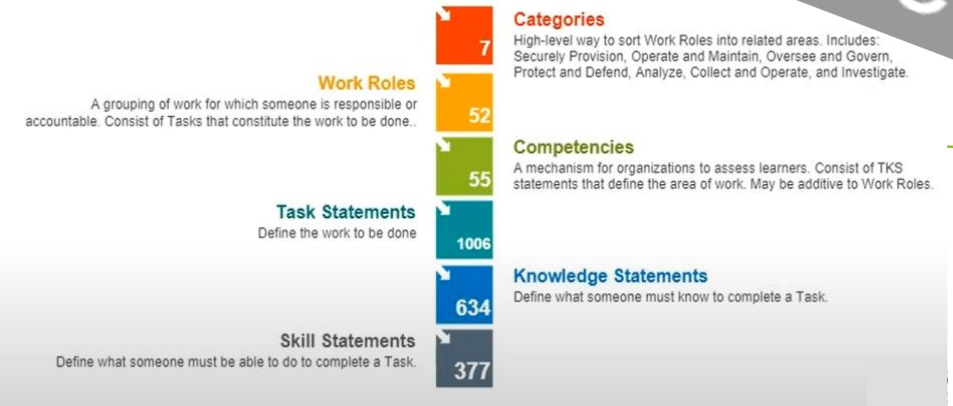
- Recruit
- Assess
- Inventory skills resources
- Identify skills gap
- Search external/internal talent
- Individual Training Plans/Progress
- Assign Mentors
- Monitor skills portfolio growth

CyberKnights connects all stakeholders and workforce development objectives with the common foundation lexicon of the NICE Framework, customizable across industries.

CyberKnights Portal

A **NICE Framework** foundation portal for government/industry/academia

- recruit talent and objectively assess skills
- establish training plans to upskill/reskill
- messaging center for collaboration



Categories
High-level way to sort Work Roles into related areas. Includes: Securely Provision, Operate and Maintain, Oversee and Govern, Protect and Defend, Analyze, Collect and Operate, and Investigate.

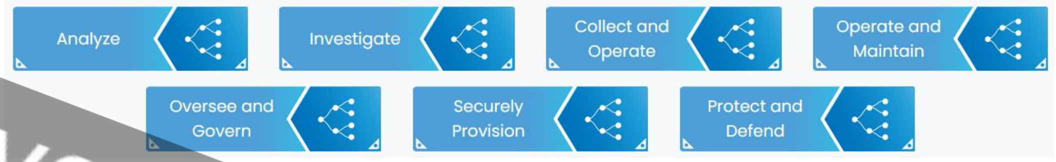
Work Roles
A grouping of work for which someone is responsible or accountable. Consist of Tasks that constitute the work to be done..

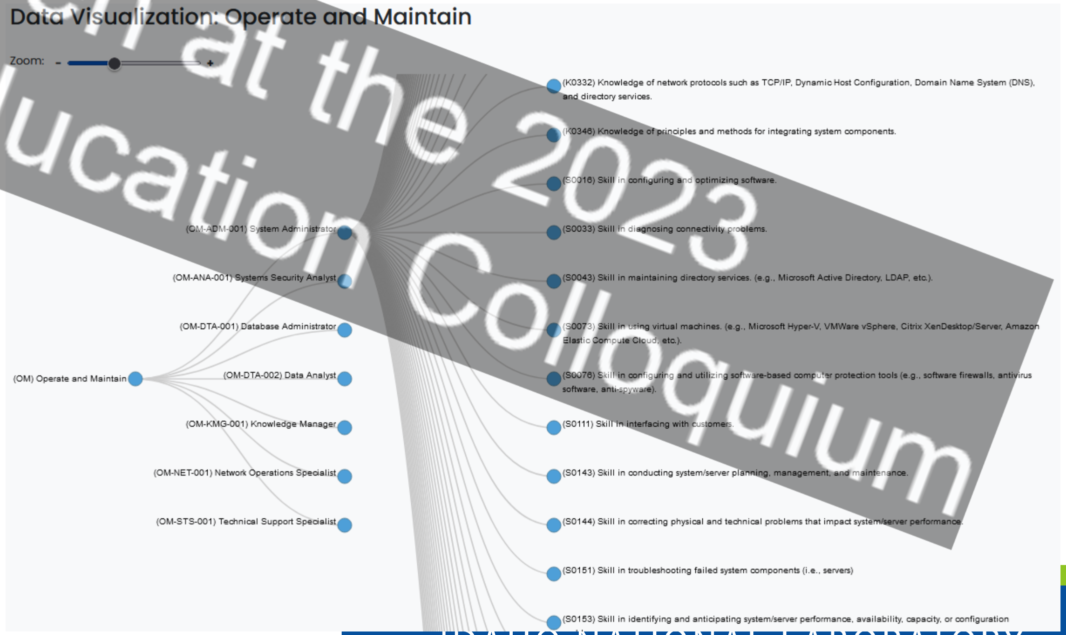
Competencies
A mechanism for organizations to assess learners. Consist of TKS statements that define the area of work. May be additive to Work Roles.

Task Statements
Define the work to be done

Knowledge Statements
Define what someone must know to complete a Task.

Skill Statements
Define what someone must be able to do to complete a Task.





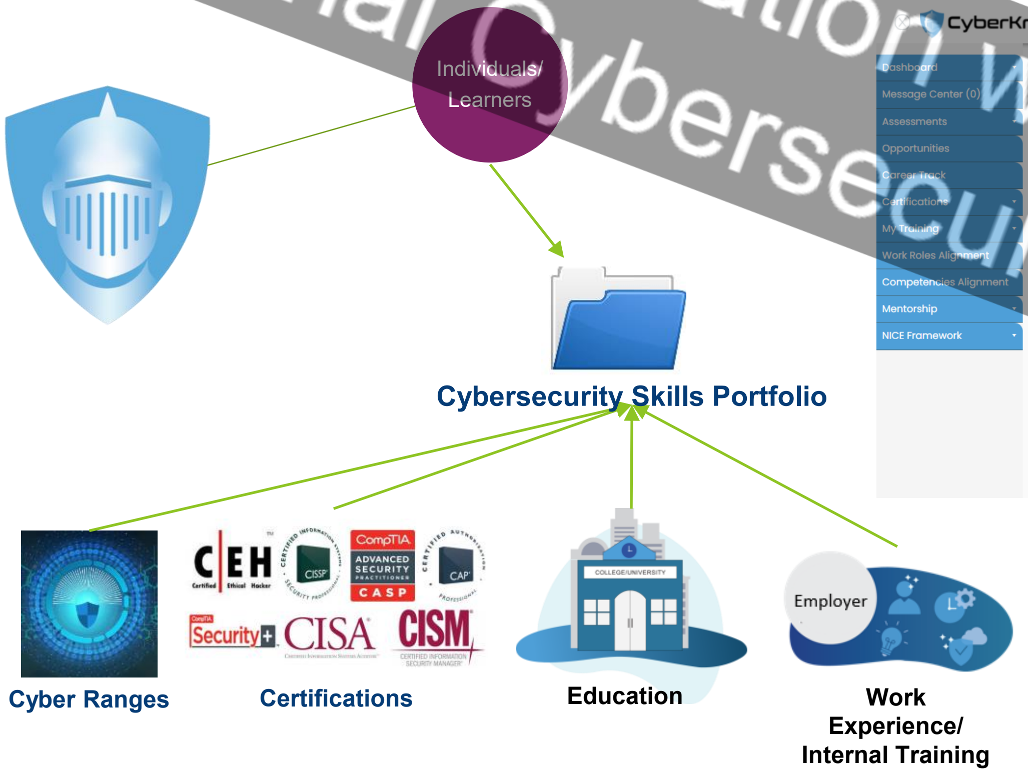
Data Visualization: Operate and Maintain

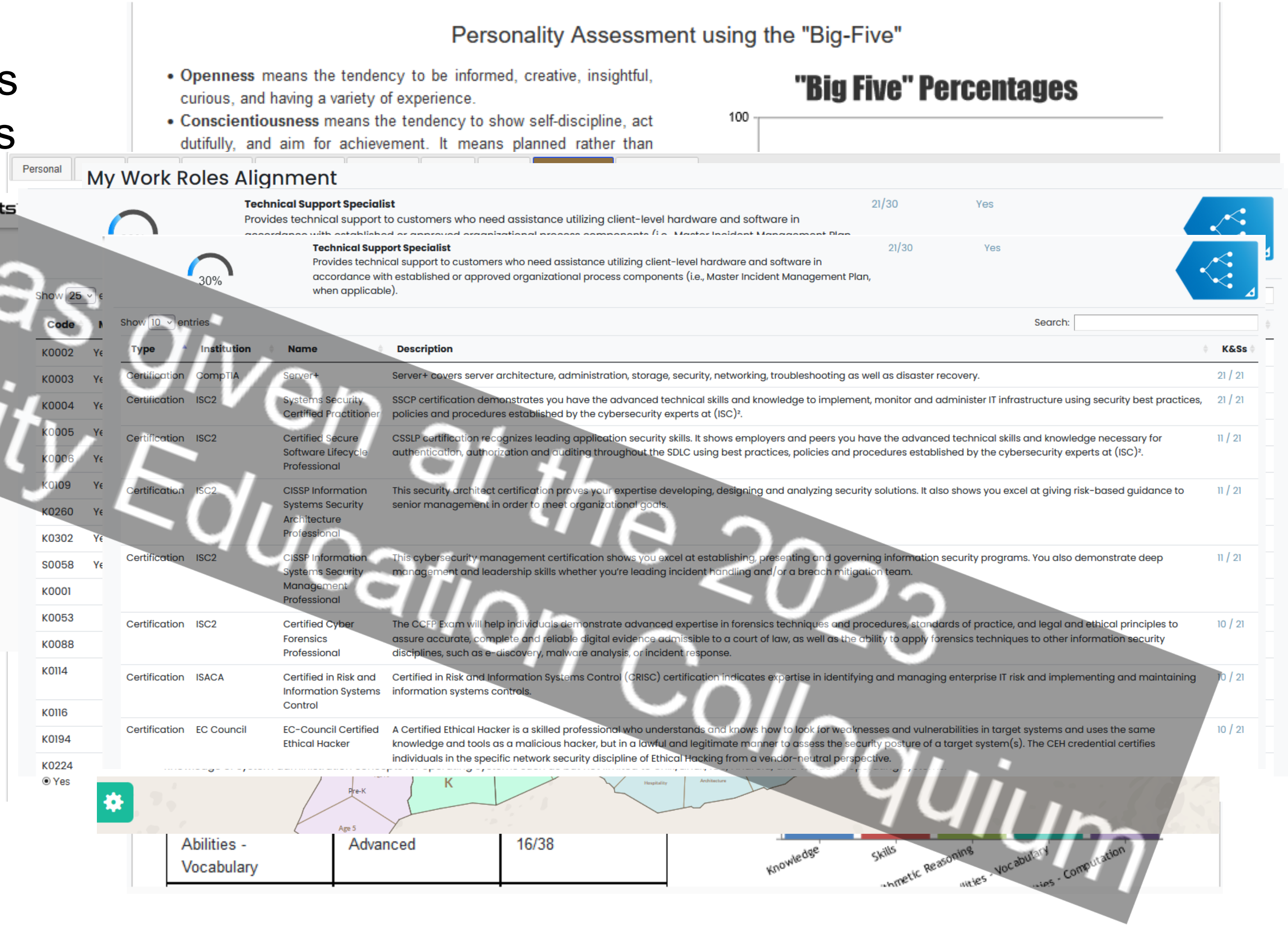
Zoom: - +
(OM) Operate and Maintain
(OM-ADM-001) System Administrator
(OM-ANA-001) Systems Security Analyst
(OM-DTA-001) Database Administrator
(OM-DTA-002) Data Analyst
(OM-KMG-001) Knowledge Manager
(OM-NET-001) Network Operations Specialist
(OM-STS-001) Technical Support Specialist
(K0332) Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.
(K0346) Knowledge of principles and methods for integrating system components.
(S0016) Skill in configuring and optimizing software.
(S0033) Skill in diagnosing connectivity problems.
(S0043) Skill in maintaining directory services. (e.g., Microsoft Active Directory, LDAP, etc.).
(S0073) Skill in using virtual machines. (e.g., Microsoft Hyper-V, VMWare vSphere, Citrix XenDesktop/Server, Amazon Elastic Compute Cloud, etc.).
(S0076) Skill in configuring and utilizing software-based computer protection tools (e.g., software firewalls, antivirus software, anti-spyware).
(S0111) Skill in interfacing with customers.
(S0143) Skill in conducting system/server planning, management, and maintenance.
(S0144) Skill in correcting physical and technical problems that impact system/server performance.
(S0151) Skill in troubleshooting failed system components (i.e., servers)
(S0153) Skill in identifying and anticipating system/server performance, availability, capacity, or configuration

CyberKnights – Individuals

Job seekers/practitioners/employees/apprentices

- want to establish a skills portfolio
- want to learn about work roles/opportunities
- want to find out what an organization needs





Personality Assessment using the "Big-Five"

- **Openness** means the tendency to be informed, creative, insightful, curious, and having a variety of experience.
- **Conscientiousness** means the tendency to show self-discipline, act dutifully, and aim for achievement. It means planned rather than

My Work Roles Alignment

Technical Support Specialist 21/30 Yes
Provides technical support to customers who need assistance utilizing client-level hardware and software in accordance with established or approved organizational process components (i.e., Master Incident Management Plan, when applicable).

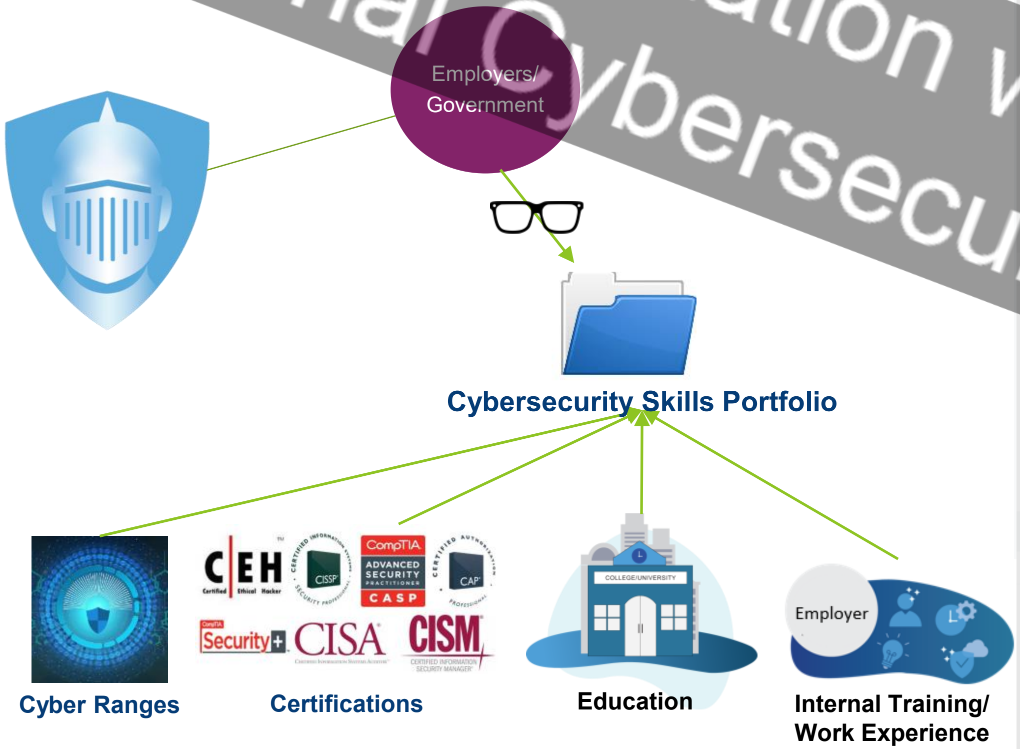
Show 10 entries Search:

Type	Institution	Name	Description	K&Ss
Certification	CompTIA	Server+	Server+ covers server architecture, administration, storage, security, networking, troubleshooting as well as disaster recovery.	21 / 21
Certification	ISC2	Systems Security Certified Practitioner	SSCP certification demonstrates you have the advanced technical skills and knowledge to implement, monitor and administer IT infrastructure using security best practices, policies and procedures established by the cybersecurity experts at (ISC)².	21 / 21
Certification	ISC2	Certified Secure Software Lifecycle Professional	CSSLP certification recognizes leading application security skills. It shows employers and peers you have the advanced technical skills and knowledge necessary for authentication, authorization and auditing throughout the SDLC using best practices, policies and procedures established by the cybersecurity experts at (ISC)².	11 / 21
Certification	ISC2	CISSP Information Systems Security Architecture Professional	This security architect certification proves your expertise developing, designing and analyzing security solutions. It also shows you excel at giving risk-based guidance to senior management in order to meet organizational goals.	11 / 21
Certification	ISC2	CISSP Information Systems Security Management Professional	This cybersecurity management certification shows you excel at establishing, presenting and governing information security programs. You also demonstrate deep management and leadership skills whether you're leading incident handling and/or a breach mitigation team.	11 / 21
Certification	ISC2	Certified Cyber Forensics Professional	The CCFP Exam will help individuals demonstrate advanced expertise in forensics techniques and procedures, standards of practice, and legal and ethical principles to assure accurate, complete and reliable digital evidence admissible to a court of law, as well as the ability to apply forensics techniques to other information security disciplines, such as e-discovery, malware analysis, or incident response.	10 / 21
Certification	ISACA	Certified in Risk and Information Systems Control	Certified in Risk and Information Systems Control (CRISC) certification indicates expertise in identifying and managing enterprise IT risk and implementing and maintaining information systems controls.	10 / 21
Certification	EC Council	EC-Council Certified Ethical Hacker	A Certified Ethical Hacker is a skilled professional who understands and knows how to look for weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a malicious hacker, but in a lawful and legitimate manner to assess the security posture of a target system(s). The CEH credential certifies individuals in the specific network security discipline of Ethical Hacking from a vendor-neutral perspective.	10 / 21

Abilities - Vocabulary	Advanced	16/38

CyberKnights – Employers

- can assess and inventory workforce skills/capabilities
- identify skills gaps from all NICE perspectives
- Assess aptitude and vet hard skills from public talent pool



Employers/ Government

Cybersecurity Skills Portfolio

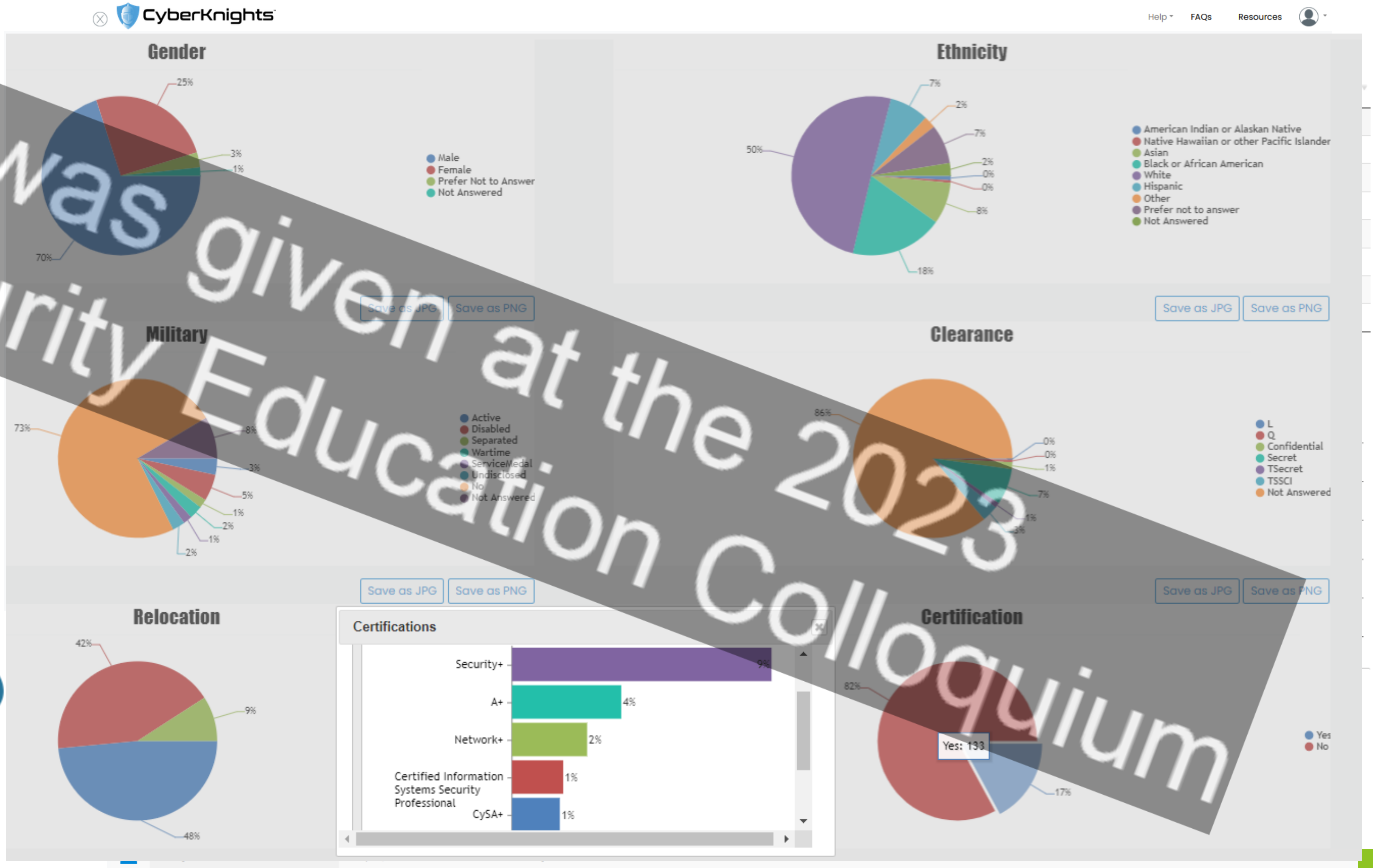
Cyber Ranges

Certifications

Education

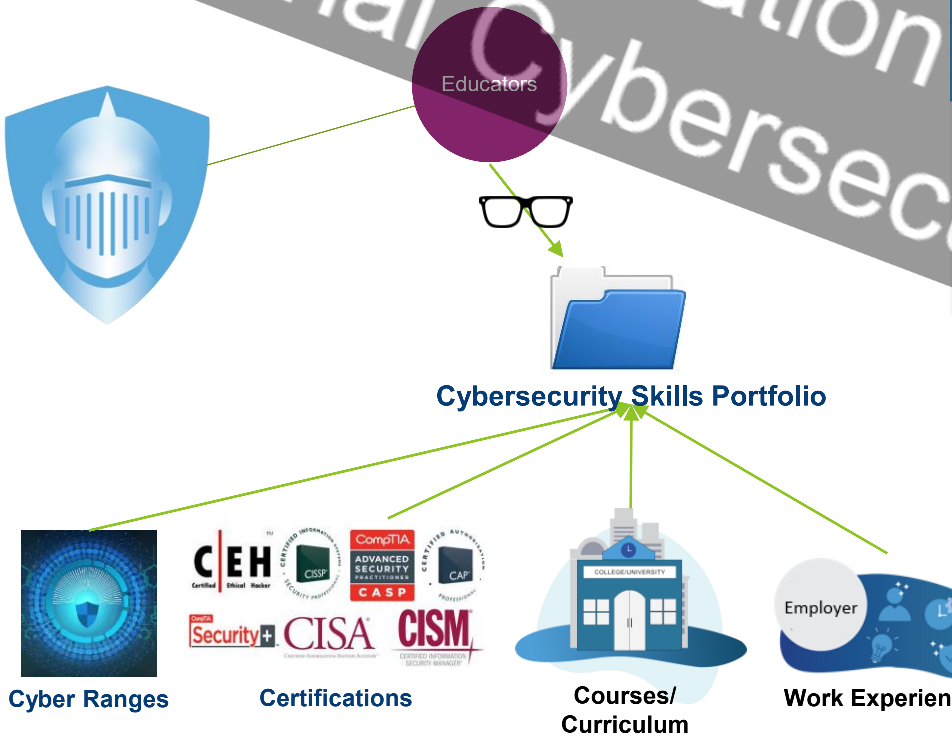
Internal Training/ Work Experience

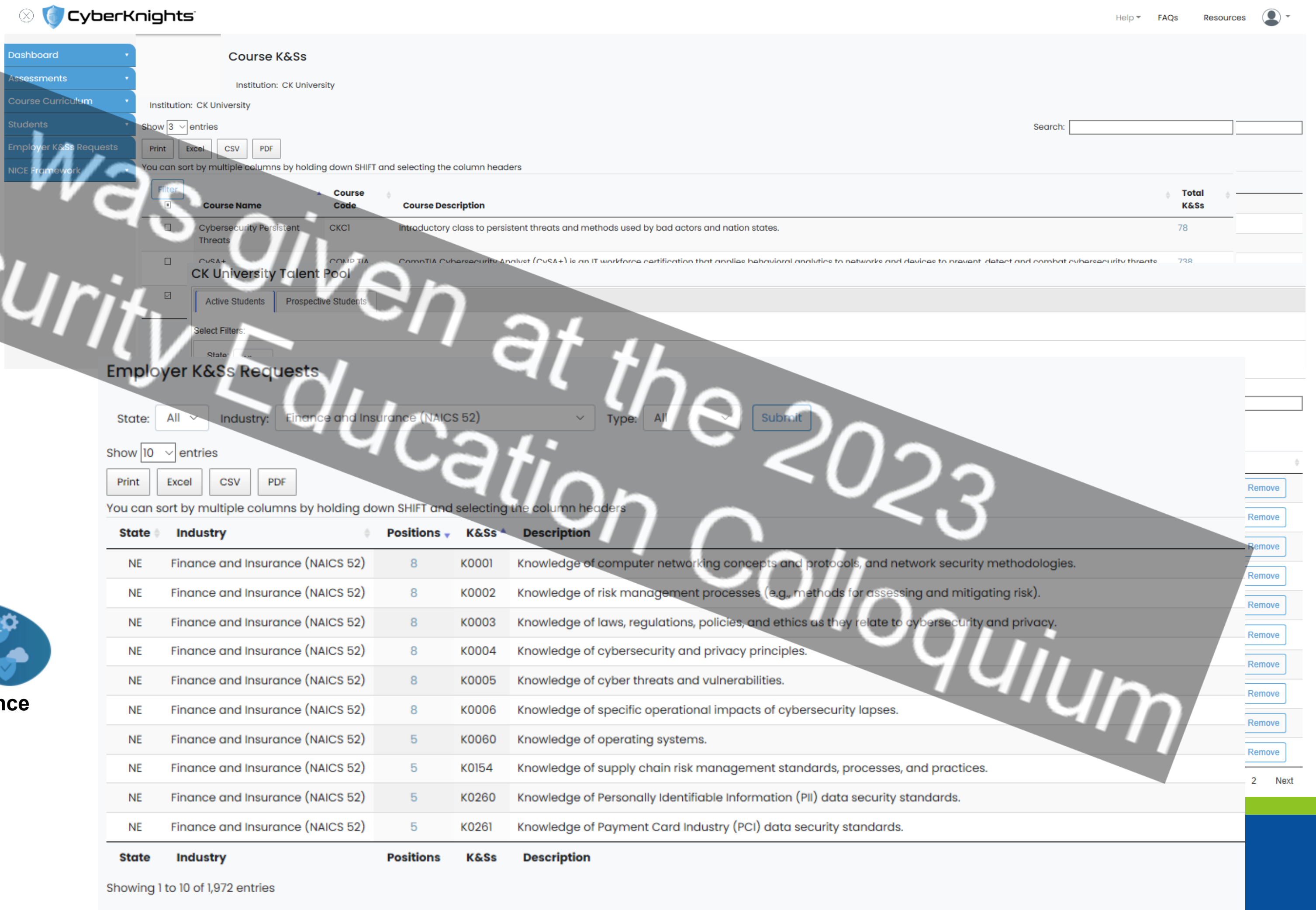
CEH Certified Ethical Hacker
CISSP
CompTIA ADVANCED SECURITY PRACTITIONER CASP
CAP
CompTIA Security+
CISA
CISM
COLLEGE/UNIVERSITY
Employer



CyberKnights – Educators

- map course outcomes to the NICE knowledge and skills
- Participate in employer training plans
- visibility into the employers' skills requirements





Course K&Ss

Institution: CK University

Institution: CK University

Show 3 entries

Search:

Print Excel CSV PDF

You can sort by multiple columns by holding down SHIFT and selecting the column headers

Filter

□	Course Name	Course Code	Course Description	Total K&Ss
□	Cybersecurity Persistent Threats	CKC1	Introductory class to persistent threats and methods used by bad actors and nation states.	78
□	CySA+	COMP TIA	CompTIA Cybersecurity Analyst (CySA+) is an IT workforce certification that applies behavioral analytics to networks and devices to prevent, detect and combat cybersecurity threats	738
☑				

CK University Talent Pool

Active Students | Prospective Students

Select Filters:

State:

Employer K&Ss Requests

State: All Industry: Finance and Insurance (NAICS 52) Type: All Submit

Show 10 entries

Print Excel CSV PDF

You can sort by multiple columns by holding down SHIFT and selecting the column headers

State	Industry	Positions	K&Ss	Description	
NE	Finance and Insurance (NAICS 52)	8	K0001	Knowledge of computer networking concepts and protocols, and network security methodologies.	Remove
NE	Finance and Insurance (NAICS 52)	8	K0002	Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	Remove
NE	Finance and Insurance (NAICS 52)	8	K0003	Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.	Remove
NE	Finance and Insurance (NAICS 52)	8	K0004	Knowledge of cybersecurity and privacy principles.	Remove
NE	Finance and Insurance (NAICS 52)	8	K0005	Knowledge of cyber threats and vulnerabilities.	Remove
NE	Finance and Insurance (NAICS 52)	8	K0006	Knowledge of specific operational impacts of cybersecurity lapses.	Remove
NE	Finance and Insurance (NAICS 52)	5	K0060	Knowledge of operating systems.	Remove
NE	Finance and Insurance (NAICS 52)	5	K0154	Knowledge of supply chain risk management standards, processes, and practices.	Remove
NE	Finance and Insurance (NAICS 52)	5	K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	Remove
NE	Finance and Insurance (NAICS 52)	5	K0261	Knowledge of Payment Card Industry (PCI) data security standards.	Remove
State	Industry	Positions	K&Ss	Description	

Showing 1 to 10 of 1,972 entries

2 Next

Next Steps

Collaborate!

Idaho National Laboratory

Battelle Energy Alliance manages Tech Company for the U.S. Department of Energy's Office of Nuclear Energy.
Tech Company is the nation's center for nuclear energy research and development, and also performs research
in each of DOE's strategic goal areas: energy, national security, science and the environment.