Interagency Committee for Apprenticeship (IACA)
Occupational Framework for Registered Apprenticeship

March 5, 2021,

Dear Information Technology (IT) Colleagues,

Rapidly advancing technology, tremendous economic change, and COVID-19 pandemic response have moved workers online and increased the need for a prepared IT workforce. This is true across economic sectors with employers seeking to hire qualified and skilled employees.

Unfortunately, workforce gaps remain in essential IT positions like data analyst, networks, and cybersecurity. Industry and technology-based occupations seek a match with skilled workforce; but significant challenges remain to finding and hiring qualified talent. One particular challenge is understanding currently needed high demand skills that would make a difference in providing a talent pool of numerous prospective new employees for your organization. We request your feedback and insight as an IT subject matter expert to help us meet these challenges.

The California Interagency Advisory Committee on Apprenticeship (IACA) IT Subcommittee represents education, training providers, and industry. We focus on leveraging registered apprenticeships to support high demand IT talent workforce needs.

We have developed key Model Industry Training Competencies (MITCs) to better align education/training programs with labor market needs. Attached is a survey which includes MITCs for data analyst (big data) and cybersecurity analyst occupations found across California for your review. We seek your input on the skills and competencies you seek in prospective employees. What knowledge and abilities are valued by today's IT employer/industry?

Please complete the survey to share whether you agree or disagree with the skills and competencies identified. We encourage you to leave comments and suggestions. We anticipate the survey to take approximately 15 minutes of your time and remain open through May 5, 2021.

Thank you very much for your feedback and suggestions!

Comments and Suggestions: We seek IT industry feedback on the following questions:

Question #1: Do you agree/disagree with the skills and competencies identified on the MITCs below?

MITC	Strongly Agree	Agreed	Neutral	Disagree	Strongly Disagree
Data Analyst	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Cybersecurity Analyst	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.

Question #2: Do you have any comments, suggestions, feedback to make regarding the MITC provided? Anything missing or require further clarification?

Click or tap here to enter text.

Question #3: Do you have any suggestions to make regarding additional competencies/skills to include that your fit your specific industry/employer needs?

Click or tap here to enter text.

Question #4: What is your sense of professional industry/employer support for these MITCs andthe registered apprenticeship workforce development model?

Click or tap here to enter text.

Your input is deeply appreciated and thanks for your participation! Please return feedback to kclement@mail.fresnostate.edu and TArefain@dir.ca.gov by **May 5, 2021** so we can finish the proposed MITC templates and distribute across California industry and employers.

If you have any additional questions, comments, or suggestions on these MITCs or ways to alignand implement a registered apprenticeships solution at your place of business, feel free to reach out to us at the above e-mail addresses.

Thank you for your time and feedback.

Your input is deeply appreciated and thanks for your participation! Please return feedback to kclement@mail.fresnostate.edu and TArefain@dir.ca.gov by **May 5, 2021** so we can finish the proposed MITC templates and distribute across California industry and employers.

If you have any additional questions, comments, or suggestions on these MITCs or ways to align and implement a registered apprenticeships solution at your place of business, feel free to reach out to us at the above e-mail addresses.

Thank you for your time and feedback.

Best regards,

Best regards,

- Dr. Keith Clement, Professor, Fresno State and IACA IT Subcommittee Chair
- Tsegay Arefaine, Strategic Business Advisor, Division of Apprenticeship (DAS)

Data Analyst MITC Developed by:

- Annie Tahitinen, Director of Technology Programs, JVS
- Michael Specchierla, Executive Director, SLOCOE, SLO Partners

Cybersecurity Analyst MITC Developed by:

- Olivia Herriford, Regional Director, Employer Engagement, ICT Digital Media Sector, Hosted by Diablo Valley College

DRAFT TEMPLATE v.6
Interagency Committee for Apprenticeship (IACA)
Occupational Framework for Registered Apprenticeship

Name of Subcommittee:	Click or tap here to enter text.
Occupation	Information Security Analyst
Job titles	Cybersecurity Support Technician
O*NET Codes (include for each job title)	15-1122.00
RAPIDS Codes	2050CB
Created	November 2020
Revision Timeline	

EEO CONSIDERATIONS

Include here considerations to expand access to the proposed apprenticeable occupation(s) for California's historically underrepresented and underutilized populations through strategic outreach, recruitment, selection, use of pre-apprentice linkage and/or other support. This may include:

1. *Description of key barriers to entry and/or advancement in this proposed apprenticeable occupation(s) for California's historically underrepresented and underutilized populations.*
2. *Description of internal processes that ensure equity and inclusion in access and promotion for this proposed apprenticeable occupation(s) for California's historically underrepresented and underutilized populations.*
3. *Identification of relevant pre-apprentice linkage agreements.*
4. *Any relevant participant reporting showing inclusion rates of underrepresented and underutilized populations.*

This statement should be reviewed by the EEOC and Pre-Apprenticeship Subcommittees before submission to IACA.

1. LENGTH OF TRAINING

Minimum length of program and hours of OJT

Type	**Hours**
Classroom Training	210
On-the-job Training	2800
Total Hours	3010

2. PROGRAM TYPE

Detail industry definition and criteria for "Competency-Based" and "Hybrid" programs for this

occupation.

☐ Competency-Based

☑ Hybrid

Comments: Adaptable for competency-based

3. CERTIFICATIONS, LICENSURE, AND OTHER CREDENTIAL REQUIREMENTS

List of credential details including Earned Before, During or After Apprenticeship. This should include identifying licensure requirements for occupations in information technology and other industries where there is DCA oversight.

Certification Name	**Type**	**Credentialing Agency(s)**
Network+	Before	CompTIA
Security+	Before	CompTIA
Linux+	Before/During	CompTIA
CySA+	During/After	CompTIA
PenTest+	During/After	CompTIA
CISSP Associate	After	$(ISC)^2$

4. **JOB FUNCTION 1: Assists in developing security policies and protocols; assists in enforcing company compliance with network security policies and protocols**

Competencies	**Core or Optional**	**RSI (classroom)**	**OJT (work-based)**	**Type of Test**
Locates (in Intranet, employee handbook or security protocols) organizational policies intended to maintain security and minimize risk and explains their use.	Core	No	Yes	
Provides guidance to employees on how toaccess networks, set passwords, reduce security threats and provide defensive measures associated with searches, software downloads, email, Internet, add-ons, software coding and transferred files.	Optional	Yes	Yes	

Competencies	Core or Optional	RSI (classroom)	OJT (work-based)	Type of Test
Ensures that password characteristicsare explained and enforced and that updates are required and enforced based on appropriate time intervals	Core	No	Yes	
Explains company or organization's policies regarding the storage, use andtransfer of sensitive data, including intellectual property and personally identifiable information. Identifies data life cycle, data	Core	No	Yes	
Assigns individuals to the appropriatepermission or access level to control access to certain web IP addresses, information and the ability to download programs and transfer data to various locations	Optional	Yes	Yes	
Assists employees in the use of technologies that restrict or allow forremote access to the organization's information technology network	Core	Yes	Yes	
Develops security compliance policies and protocols for external services (i.e.Cloud service providers, software services, external data centers)	Optional	Yes	Yes	
Complies with incident response and handling methodologies	Optional	Yes	Yes	
Articulates the business need or mission of the organization as it pertains to the use of IT systems and the storage of sensitive data	Core	No	Yes	

5. **JOB FUNCTION 2: Provides technical support to users or customers**

Competencies	Core or Optional	RSI (classroom)	OJT (work-based)	Type of Test
Manages inventory of IT resources	Core	No	Yes	
Diagnoses and resolves customer-reported system incidents	Core	Yes	Yes	
Installs and configures hardware, software and peripheral equipment for system users	Core	No	Yes	
Monitors client-level computer system performance	Core	No	Yes	
Tests computer system performance	Core	No	Yes	
Troubleshoots system hardware and software	Core	No	Yes	
Administers accounts, network rights, and access to systems and equipment	Core	No	Yes	
Implements security measures for usesin system and ensures that system designs incorporate security configuration guidelines	Optional	Yes	Yes	

6. **JOB FUNCTION 3: Installs, configures, tests, operates, maintains and manages networks and their firewalls including hardware and software that permit sharing and transmission of information**

Competencies	Core or Optional	RSI (classroom)	OJT (work-based)	Type of Test
Collaborates with system developers and users to assist in the selection of appropriate design solutions to ensurethe compatibility of system components	Core	No	Yes	
Installs, replaces, configures and optimizes network hubs, routers and switches	Optional	Yes	Yes	
Assists in network backup and recovery procedures	Core	No	Yes	
Diagnoses network connectivity problems	Core	Yes	Yes	

Competencies	Core or Optional	RSI (classroom)	OJT (work-based)	Type of Test
Modifies network infrastructure toserve new purposes or improve workflow	Optional	No	Yes	
Integrates new systems into existing network architecture	Core	Yes	Yes	
Patches network vulnerabilities to ensure information is safeguarded against outside parties	Core	Yes	Yes	
Tests and maintains network infrastructure including software and hardware devices	Core	Yes	Yes	
Establishes adequate access controlsbased on principles of least privilege and need-to-know	Core	Yes	Yes	
Implements security measures for users in system and ensures that system designs incorporate security configuration guidelines	Core	No	Yes	

7. **JOB FUNCTION 4: Installs, configures, troubleshoots and maintains server configurations to ensure their confidentiality, integrity and availability; also manages accounts, firewalls, configuration, patch and vulnerability management. Is responsible for access control, security configuration and administration**

Competencies	Core or Optional	RSI (classroom)	OJT (work-based)	Type of Test
Checks system hardware availability, functionality, integrity and efficiency	Core	No	Yes	
Conducts functional and connectivitytesting to ensure continuing operability	Core	No	Yes	
Conducts periodic server maintenanceincluding cleaning (physically and electronically), disk checks, system configuration and monitoring, data downloads, backups and testing	Core	No	Yes	

Competencies	Core or Optional	RSI (classroom)	OJT (work-based)	Type of Test
Assists in the development of group policies and access control lists to ensure compatibility with organizational standards, business rules and needs	Optional	No	Yes	
Documents compliance with or changes to system administration standard operating procedures	Core	No	Yes	
Maintains baseline system security according to organizational policies	Core	No	Yes	
Manages accounts, network rights and access to systems and equipment	Core	Yes	Yes	
Monitors and maintains server configuration	Core	Yes	Yes	
Supports network components	Core	No	Yes	
Diagnoses faulty system/server hardware; seeks appropriate support or assistance to perform server repairs	Core	No	Yes	
Verifies data redundancy and system recovery procedures	Core	Yes	Yes	
Assists in the coordination or installation of new or modified hardware, operating systems and other baseline software	Core	Yes	Yes	
Provides ongoing optimization and problem-solving support	Core	No	Yes	
Resolves hardware/software interface and interoperability problems	Core	Yes	Yes	

8. **JOB FUNCTION 5: Configures tools and technologies to detect, mitigate and prevent potential threats**

Competencies	Core or Optional	RSI (classroom)	OJT (work-based)	Type of Test
Installs and maintains cyber securitydetection, monitoring and threat management software	Core	Yes	Yes	
Coordinates with network administrators to administer the updating of rules and signatures for intrusion/detection protection systems, anti-virus and network black and white list	Core	No	Yes	
Manages IP addresses based on current threat environment	Core	Yes	Yes	
Ensures application of security patches for commercial products integratedinto system design	Core	No	Yes	
Uses computer network defense toolsfor continual monitoring and analysis of system activity to identify malicious activity	Optional	Yes	Yes	

9. **JOB FUNCTION 6: Assesses and mitigates system network, business continuity and related security risks and vulnerabilities**

Competencies	Core or Optional	RSI (classroom)	OJT (work-based)	Type of Test
Applies security policies to meet security objectives of the system	Core	No	Yes	
Performs system administration to ensure current defense applicationsare in place, including on Virtual Private Network devices	Core	Yes	Yes	
Ensures that data back up and restoration systems are functional andconsistent with company's document retention policy and business continuity needs	Core	No	Yes	
Identifies potential conflicts with implementation of any computer network defense tools. Performs tool signature testing and optimization	Optional	Yes	Yes	

Competencies	Core or Optional	RSI (classroom)	OJT (work-based)	Type of Test
Installs, manages and updates intrusion detection system	Optional	Yes	Yes	
Performs technical and non-technicalrisk and vulnerability assessments of relevant technology focus areas	Optional	Yes	Yes	
Conducts authorized penetration testing (Wi-Fi, network perimeter,application security, cloud, mobile devices) and assesses results	Core	Yes	Yes	
Documents systems security operations and maintenance activities	Core	No	Yes	
Communicates potential risks orvulnerabilities to manager. Collaborates with others to recommend vulnerability corrections	Optional	No	Yes	
Identifies information technology security program implications of newtechnologies or technology upgrades	Optional	Yes	Yes	

10. **JOB FUNCTION 7: Reviews network utilization data to identify unusual patterns, suspicious activity or signs of potential threats**

Competencies	Core or Optional	RSI (classroom)	OJT (work-based)	Type of Test
Identifies organizational trends with regard to the security posture of systems; identifies unusual patterns or activities	Core	Yes	Yes	
Characterizes and analyzes networktraffic to identify anomalous activityand potential threats; performs computer network defense trend analysis and reporting	Optional	Yes	Yes	
Receives and analyzes network alertsfrom various sources within the enterprise and determines possible causes of such alerts	Optional	No	Yes	
Runs tests to detect real or potential threats, viruses, malware, etc.	Optional	Yes	Yes	

Competencies	Core or Optional	RSI (classroom)	OJT (work-based)	Type of Test
Assists in researching cost-effective security controls to mitigate risks	Core	No	Yes	
Helps perform damage assessments in the event of an attack	Optional	Yes	Yes	
Monitors network data to identify unusual activity, trends, unauthorizeddevices or other potential vulnerabilities	Optional	Yes	Yes	
Documents and escalates incidentsthat may cause immediate or long-term impact to the environment	Core	No	Yes	
Provides timely detection, identification and alerts of possibleattacks and intrusions, anomalous activities, and distinguish these incidents and events from normal baseline activities	Optional	Yes	Yes	
Uses network monitoring tools to capture and analyze network traffic associated with malicious activity	Optional	Yes	Yes	
Performs intrusion analysis	Optional	Yes	Yes	
Sets containment blockers to alignwith company policy regarding computer use and web access	Core	No	Yes	

11. **JOB FUNCTION 8: Responds to cyber intrusions and attacks and provides defensive strategies**

Competencies	Core or Optional	RSI (classroom)	OJT (work-based)	Type of Test
Assists in the development of appropriate courses of action in response to identified anomalous network activity	Optional	Yes	Yes	
Triages systems operations impact: malware, worms, man-in-the-middleattack, denial of service, rootkits, keystroke loggers, SQL injection and cross-site scripting	Optional	Yes	Yes	
Reconstructs a malicious attack or activity based on network traffic	Optional	Yes	Yes	
Correlates incident data to identifyspecific vulnerabilities and make recommendations that enable expeditious remediation	Optional	No	Yes	
Monitors external data sources to maintain currency of Computer Network Defense threat condition anddetermines which security issues may have an impact on the enterprise. Performs file signature analysis	Optional	Yes	Yes	
Performs analysis of log files from a variety of sources to identify threats tonetwork security; performs file signature analysis	Optional	Yes	Yes	
Performs computer network defense incident triage to include determiningscope, urgency and potential impact; identifies the specific vulnerability; provides training recommendations; and makes recommendations that enable expeditious remediation	Optional	No	Yes	
Receives and analyzes network alertsfrom various sources within the enterprise and determines possible causes of such alerts	Optional	Yes	Yes	
Tracks and documents computer network defense incidents from initial detection through final resolution	Core	Yes	Yes	

Competencies	Core or Optional	RSI (classroom)	OJT (work-based)	Type of Test
Collects intrusion artifacts and uses discovered data to enable mitigationof potential computer network defense (CND) incidents	Optional	No	Yes	
Performs virus scanning on digital media	Core	Yes	Yes	

LIST OF NAMES OF SUB-COMMITTEE MEMBERS

Must include industry representatives of employers and employees.

Dr. Keith Clement
Kenneth Anwanyu
Miriam Farnbauer
Olivia Herriford
Keith Koo
Michael Speccheria
Meredith Stowell
Annie Tahtinen
Katherine Webster

Comments, Suggestions, and Feedback