Appendix A

CYBERSECURITY PROFESSIONAL

WORK PROCESS SCHEDULE

AND

RELATED INSTRUCTION OUTLINE

Appendix A

WORK PROCESS SCHEDULE
CYBERSECURITY PROFESSIONAL

O*NET-SOC CODE: 15-1212.00 **RAPIDS CODE:** 2050CB

This schedule is attached to and a part of these Standards for the above identified occupation.

1. APPRENTICESHIP APPROACH

☐ Time-based ☒ Competency-based ☐ Hybrid

2. TERM OF APPRENTICESHIP

The term of **Cybersecurity Professional** is **Competency Based** supplemented by the minimum required **144** hours of related training instruction per year.

3. RATIO OF APPRENTICES TO JOURNEYWORKERS

The apprentice to journeyworker ratio is: 1 Apprentice(s) to 1 Journeyworker(s).

4. APPRENTICE WAGE SCHEDULE

Apprentices shall be paid a progressively increasing schedule of wages based on either a percentage or a dollar amount of the current hourly journeyworker wage rate, which is: $35.00/per hour.

Period	Wage (Hourly)	Description
1	$16.00	6 months + hours
2	$16.50	6 months + hours
3	$17.00	6 months + hours
4	$17.50	6 months + hours

5. PROBATIONARY PERIOD

Applicants selected for apprenticeship will serve a probationary period of **1000** hours.

6. SELECTION PROCEDURES

Applicants will be selected by individual participating employer sponsors using selection method #_4, as outlined in the California Code of Regulations, Title 8, Chapter 2, Part 1, Section 215, Chapter 6, from a pool of eligible created during the established recruiting process in accordance with the State and Federal

Equal Opportunity regulations.

1. Minimum age of all applicants shall be 16 years. There is no maximum age;
2. Educational prerequisite for entry: High school diploma or GED/equivalent;
3. Physical prerequisites: Applicant must have the ability to safely perform the work of the trade/occupation. Physical examination required for entry is at no cost to the applicant and the physical exam will be defined by the individual employer sponsor.
4. Written Test: Administered by Faculty and/or Program Coordinator
5. Oral Interview: None Required
6. All applicants will be notified in writing of Acceptance or Rejection.
7. If rejected, reasons for rejections will be stated.
8. A pool of applicants will be established and maintained for two years as follows:
    a. Interested applicants will have an opportunity to attend a public orientation and enroll in the program's employment preparation course. Completers of the course will be guided through the development of a resume and job application, which will be published to participating employer partners.
9. And applicants will be employed as follows:
    a. Applicants will follow directives of individual employer partners through job application, interview and pre-screening.
    b. Applicant's prior work experience and training will be evaluated by the committee at the time of registration, and appropriate credit will be given toward a higher apprenticeship and/or wage bracket. Apprentice applicant must verify, in writing, all past experience/education for consideration of credit.
    c. Each participating employer sponsor, upon determination of the need to employ and train an apprentice, will register an apprentice after upholding a fair and consistent sourcing, recruiting, and evaluation process;
    d. Participating employer sponsors will report recruitment and selection data annually to the Program Name Apprenticeship Training Program coordinator/director;
    e. Minimum age of all applicants shall be 16 years. There is no maximum age;
    f. Educational prerequisite for entry: High school diploma or GED/equivalent;
    g. Physical prerequisites: Applicant must have the ability to safely perform the work of the trade/occupation. Physical examination required for entry is at no cost to the applicant and the physical exam will be defined by the individual employer sponsor.
    h. Drug screening prior to employment, as well as random drug screening throughout the apprenticeship program may be required for selection and/or continued participation/employment;
    i. General aptitude or other skills test shall be defined by the individual employer sponsor and administered by the employer sponsor or its delegated agent;
    j. Oral interview is per employer sponsor's individual selection procedures with selection documentation to be on file with the Program Name program director/coordinator

WORK PROCESS SCHEDULE
CYBERSECURITY PROFESSIONAL

O*NET-SOC CODE: 15-1212.00 **RAPIDS CODE:** 2050CB

On-the-Job Learning Outline

IT Project Management Work Processes		
Competencies	**Date Completed**	**Initial**
A. Perform needs analysis to determine opportunities for new and improved business process solutions.		
B. Provide advice on project costs, design concepts, or design changes.		
C. Provide enterprise cybersecurity and supply chain risk management guidance for development of the Continuity of Operations Plans.		
D. Resolve conflicts in laws, regulations, policies, standards, or procedures.		
E. Review or conduct audits of information technology (IT) programs and projects.		
F. Evaluate the effectiveness of procurement function in addressing information security requirements and supply chain risks through procurement activities and recommend improvements.		
G. Develop and document supply chain risks for critical system elements, as appropriate.		
H. Ensure that all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals.		
I. Act as a primary stakeholder in the underlying information technology (IT) operational processes and functions that support the service, provide direction and monitor all significant activities so the service is delivered successfully.		
J. Coordinate and manage the overall service provided to a customer end-to-end.		
K. Ensure that appropriate Service-Level Agreements (SLAs) and underpinning contracts have been defined that clearly set out for the customer a description of the service and the measures for monitoring the service.		
L. Gather feedback on customer satisfaction and internal service performance to foster continual improvement.		
M. Manage the internal relationship with information technology (IT) process owners supporting the service, assisting with the definition and agreement of Operating Level Agreements (OLAs).		
N. Review service performance reports identifying any significant issues and variances, initiating, where necessary, corrective actions and ensuring that all outstanding issues are followed up.		
O. Work with other service managers and product owners to balance and prioritize services to meet overall customer requirements, constraints, and objectives.		
P. Conduct import/export reviews for acquiring systems and software.		
Q. Develop supply chain, system, network, performance, and cybersecurity requirements.		
R. Ensure that supply chain, system, network, performance, and cybersecurity requirements are included in contract language and delivered.		
S. Identify and address cyber workforce planning and management issues (e.g. recruitment, retention, and training).		

T. Lead and oversee budget, staffing, and contracting.		
U. Draft and publish supply chain security and risk management documents.		
Database Administration Work Processes		
Competencies	**Date Completed**	**Initial**
A. Analyze and plan for anticipated changes in data capacity requirements.		
B. Maintain database management systems software.		
C. Maintain directory replication services that enable information to replicate automatically from rear servers to forward units via optimized routing.		
D. Maintain information exchanges through publish, subscribe, and alert functions that enable users to send and receive critical information as required.		
E. Manage the compilation, cataloging, caching, distribution, and retrieval of data.		
F. Monitor and maintain databases to ensure optimal performance.		
G. Perform backup and recovery of databases to ensure data integrity.		
H. Provide recommendations on new database technologies and architectures.		
I. Performs configuration management, problem management, capacity management, and financial management for databases and data management systems.		
J. Supports incident management, service-level management, change management, release management, continuity management, and availability management for databases and data management systems.		
K. Maintain assured message delivery systems.		
L. Implement data management standards, requirements, and specifications.		
M. Implement data mining and data warehousing applications.		
N. Install and configure database management systems and software.		
IT Program Audit Work Processes		
Competencies	**Date Completed**	**Initial**
A. Develop methods to monitor and measure risk, compliance, and assurance efforts.		
B. Provide ongoing optimization and problem-solving support.		
C. Provide recommendations for possible improvements and upgrades.		
D. Review or conduct audits of information technology (IT) programs and projects.		
E. Evaluate the effectiveness of procurement function in addressing information security requirements and supply chain risks through procurement activities and recommend improvements.		
F. Review service performance reports identifying any significant issues and variances, initiating, where necessary, corrective actions and ensuring that all outstanding issues are followed up.		
G. Conduct import/export reviews for acquiring systems and software.		
H. Ensure that supply chain, system, network, performance, and cybersecurity requirements are included in contract language and delivered.		

Forensic Analysis Work Processes		
Competencies	**Date Completed**	**Initial**
A. Develop a plan to investigate alleged crime, violation, or suspicious activity utilizing computers and the Internet.		
B. Establish relationships, if applicable, between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies, vendors, public relations professionals).		
C. Analyze incident data for emerging trends.		
D. Perform file and registry monitoring on the running system after identifying intrusion via dynamic analysis.		
E. Read, interpret, write, modify, and execute simple scripts (e.g., Perl, VBScript) on Windows and UNIX systems (e.g., those that perform tasks such as: parsing large data files, automating manual tasks, and fetching/processing remote data).		
F. Identify and/or develop reverse engineering tools to enhance capabilities and detect vulnerabilities.		
G. Analyze organizational cyber policy.		
Vulnerability Assessment Work Processes		
Competencies	**Date Completed**	**Initial**
A. Analyze organization's cyber defense policies and configurations and evaluate compliance with regulations and organizational directives.		
B. Conduct and/or support authorized penetration testing on enterprise network assets.		
C. Maintain deployable cyber defense audit toolkit (e.g., specialized cyber defense software and hardware) to support cyber defense audit missions.		
D. Maintain knowledge of applicable cyber defense policies, regulations, and compliance documents specifically related to cyber defense auditing.		
E. Prepare audit reports that identify technical and procedural findings and provide recommended remediation strategies/solutions.		
F. Conduct required reviews as appropriate within environment (e.g., Technical Surveillance, Countermeasure Reviews [TSCM], TEMPEST countermeasure reviews).		
G. Perform technical (evaluation of technology) and nontechnical (evaluation of people and operations) risk and vulnerability assessments of relevant technology focus areas (e.g., local computing environment, network and infrastructure, enclave boundary, supporting infrastructure, and applications).		
H. Make recommendations regarding the selection of cost-effective security controls to mitigate risk (e.g., protection of information, systems and processes).		

RELATED INSTRUCTION OUTLINE
CYBERSECURITY PROFESSIONAL

O*NET-SOC CODE: 15-1212.00 **RAPIDS CODE:** 2050CB

Through consultation with the Apprenticeship Committee and the indenturing employer, apprentices will select an applicable program of study/course track and complete a minimum of 144 hours of related instruction per year of apprenticeship. Courses will be approved by the Apprenticeship Committee and made available to applicable apprentices by approved education providers/institutions. Apprentices will enroll in, and complete, the required coursework that satisfies the minimum requirements of the program. Prior applicable education and training will be credited towards completion of related education requirements and apprentices will be offered tracks advancing their technical aptitude in the profession.

Source: California State University, San Bernardino

The following related training outline identifies the courses that are currently identified as suggested course work for this occupation:

Management of Information Technology – 45 hours

Systems Analysis & Design – 45 hours

Information Systems Planning and Policy – 45 hours

Advanced Computer Networks – 45 hours

Advanced Database Management and Information Assurance – 45 hours

Cybersecurity Management – 45 hours

Penetration Testing and Ethical Hacking – 45 hours

Enterprise System Administration – 45 hours

Incident Handling and Cyber Investigation (Digital Forensics) – 45 hours

Special Topics Course (research, web security, cloud services – 45 hours

Problem Solving and Decision Making – 45 hours

Project Management – 45 hours

This workforce product was funded by a $4,697,637 grant awarded to Riverside Community College District by the U.S. Department of Labor (DOL) – Apprenticeship Building America (ABA) Grant. The total cost of the product is financed with 100% Federal funds. The product was created by the recipient and does not necessarily reflect the official position of DOL-ETA. DOL-ETA makes no guarantees, warranties, or assurances of any kind, express or implied, with respect to such information, including any information on linked sites and including, but not limited to, accuracy of the information or its completeness, timeliness, usefulness, adequacy, continued availability, or ownership. This product is copyrighted by the institution that created it.