CYBER SECURITY WORKFORCE DEVELOPMENT FRAMEWORK

https://www.nist.gov/itl/applied-cybersecurity/nice

SECURELY PROVISION

Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development.

- **Risk Management**
  Oversees, evaluates, and supports the documentation, validation, assessment and authorization processes necessary to assure that existing and new information technology (IT) systems meet the organization's cyber security and risk requirements. Ensures appropriate treatment of risk, compliance and assurance from internal and external perspectives.
- **Software Development**
  Develops and writes/codes new (or modifies existing) computer applications, software or specialized utility programs following software assurance best practices.
- **Systems Architecture**
  Develops system concepts and works on the capabilities phases of the systems development life cycle; translates technology and environmental conditions (e.g., law and regulation) into system and security designs and processes.
- **Technology R&D**
  Conducts technology assessment and integration processes; provides and supports a prototype capability and/or evaluates its utility.
- **Systems Requirements Planning**
  Consults with customers to gather and evaluate functional requirements and translates these into technical solutions. Provides guidance to customers about applicability of information systems to meet business needs.
- **Test and Evaluation**
  Develops and conducts tests of systems to evaluate compliance with specifications and requirements by applying principles and methods for cost-effective planning, evaluating, verifying and validating of technical, functional and performance characteristics (including interoperability) of systems or elements of systems incorporating IT.
- **Systems Development**
  Works on the development phases of the systems development life cycle.

OVERSEE AND GOVERN

Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cyber security work.

- **Legal Advice and Advocacy**
  Provides legally sound advice and recommendations to leadership and staff on a variety of relevant topics within the pertinent subject domain. Advocates legal and policy changes, and makes a case on behalf of client via a wide range of written and oral work products, including legal briefs and proceedings.
- **Training, Education and Awareness**
  Conducts training of personnel within the pertinent subject domain. Develops, plans, coordinates, delivers and/or evaluates training courses, methods and techniques as appropriate.
- **Cyber Security Management**
  Oversees the cyber security program of an information system or network, including managing information security implications within the organization, specific program or other area of responsibility, to include strategic, personnel, infrastructure, requirements, policy enforcement, emergency planning, security awareness and other resources.
- **Strategic Planning and Policy**
  Develops policies and plans and/or advocates for changes in policy that support organizational cyberspace initiatives or required changes/ enhancements.
- **Executive Cyber Leadership**
  Supervises, manages and/or leads work and workers performing cyber and cyber-related and/or cyber operations work.
- **Program/Project Management and Acquisition**
  Applies knowledge of data, information, processes, organizational interactions, skills and analytical expertise, as well as systems, networks and information exchange capabilities to manage acquisition programs. Executes duties governing hardware, software, and information system acquisition programs and other program management policies. Provides direct support for acquisitions that use information technology (IT) (including National Security Systems), applying IT-related laws and policies, and provides IT-related guidance throughout the total acquisition life cycle.

PROTECT AND DEFEND

Identifies, analyzes and mitigates threats to internal information technology (IT) systems and/or networks.

- **Cyber Defense Analysis**
  Uses defensive measures and information collected from a variety of sources to identify, analyze and report events that occur or might occur within the network to protect information, information systems and networks from threats.
- **Cyber Defense Infrastructure Support**
  Tests, implements, deploys, maintains, reviews and administers the infrastructure hardware and software that are required to effectively manage the computer network, defense service provider network and resources. Monitors network to actively remediate unauthorized activities.
- **Incident Response**
  Responds to crises or urgent situations within the pertinent domain to mitigate immediate and potential threats. Uses mitigation, preparedness and response and recovery approaches, as needed, to maximize survival of life, preservation of property and information security. Investigates and analyzes all relevant response activities.
- **Vulnerability Assessment and Management**
  Conducts assessments of threats and vulnerabilities; determines deviations from acceptable configurations, enterprise or local policy; assesses the level of risk; and develops and/or recommends appropriate mitigation countermeasures in operational and nonoperational situations.

INVESTIGATE

Investigates cyber security events or crimes related to information technology (IT) systems, networks, and digital evidence.

- **Cyber Investigation**
  Applies tactics, techniques and procedures for a full range of investigative tools and processes to include, but not limited to, interview and interrogation techniques, surveillance, counter surveillance, and surveillance detection, and appropriately balances the benefits of prosecution versus intelligence gathering.
- **Digital Forensics**
  Collects, processes, preserves, analyzes and presents computer-related evidence in support of network vulnerability mitigation and/or criminal, fraud, counterintelligence or law enforcement investigations.

NICE

National Initiative for Cybersecurity Education

Work Roles | Tasks | Skills
Knowledge | Abilities

ANALYZE

Performs highly specialized review and evaluation of incoming cyber security information to determine its usefulness for intelligence.

- **Threat Analysis**
  Identifies and assesses the capabilities and activities of cyber security criminals or foreign intelligence entities; produces findings to help initialize or support law enforcement and counterintelligence investigations or activities.
- **Exploitation Analysis**
  Analyzes collected information to identify vulnerabilities and potential for exploitation.
- **All-Source Analysis**
  Analyzes threat information from multiple sources, disciplines and agencies across the Intelligence Community. Synthesizes and places intelligence information in context; draws insights about possible implications.
- **Targets**
  Applies current knowledge of one or more regions, countries, non state entities and/or technologies.
- **Language Analysis**
  Applies language, cultural and technical expertise to support information collection, analysis and other cyber security activities.

OPERATE AND MAINTAIN

Provides the support, administration and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.

- **Data Administration**
  Develops and administers databases and/or data management systems that allow for the storage, query, protection and utilization of data.
- **Knowledge Management**
  Manages and administers processes and tools that enable the organization to identify, document and access intellectual capital and information content.
- **Customer Service and Technical Support**
  Addresses problems; installs, configures, troubleshoots, and provides maintenance and training in response to customer requirements or inquiries (e.g., tiered-level customer support). Typically provides initial incident information to the Incident Response (IR) Specialty.
- **Network Services**
  Installs, configures, tests, operates, maintains, and manages networks and their firewalls, including hardware (e.g., hubs, bridges, switches, multiplexers, routers, cables, proxy servers and protective distributor systems) and software that permit the sharing and transmission of all spectrum transmissions of information to support the security of information and information systems.
- **Systems Administration**
  Installs, configures, troubleshoots and maintains server configurations (hardware and software) to ensure their confidentiality, integrity and availability. Manages accounts, firewalls and patches. Responsible for access control, passwords and account creation and administration.
- **Systems Analysis**
  Studies an organization's current computer systems and procedures, and designs information systems solutions to help the organization operate more securely, efficiently and effectively. Brings business and information technology (IT) together by understanding the needs and limitations of both.

COLLECT AND OPERATE

Provides specialized denial and deception operations and collection of cyber security information that may be used to develop intelligence.

- **Collection Operations**
  Executes collection using appropriate strategies and within the priorities established through the collection management process.
- **Cyber Operational Planning**
  Performs in-depth joint targeting and cyber security planning processes. Gathers information and develops detailed Operational Plans and Orders supporting requirements. Conducts strategic and operational-level planning across the full range of operations for integrated information and cyber space operations.
- **Cyber Operations**
  Performs activities to gather evidence on criminal or foreign intelligence entities to mitigate possible or real-time threats, protect against espionage or insider threats, foreign sabotage, international terrorist activities, or to support other intelligence activities.

Further information regarding this poster's topic can be found on this website: *https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework* **and in this NIST Special Publication 800-181:** *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf?trackDocs=NIST.SP.800-181.pdf*