National Initiative for Cybersecurity Education (NICE)

By National Institute of Standards and Technology (NIST) U.S. Department of Commerce
National Initiative of Cyber Security Education (NICE) Framework, a Cyber Security Workforce Framework by the National Institute of Standards and Technology, is a partnership between the US Department of Commerce, Academia, and the Private sector. Its primary focus lies in developing a robust cybersecurity workforce who are experts in combating cyber threats by deploying the best practices as per the seven workforce categories mentioned below.

<table>
<thead>
<tr>
<th>Category</th>
<th>Workforce Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td>SECURELY PROVISION</td>
<td>Concept, Design, Procure, Information Technology (IT) System, Systems &amp; Network Development</td>
</tr>
<tr>
<td>OPERATE &amp; MAINTAIN</td>
<td>Support, Administrate, Maintain, Information Technology (IT) Performance, Information Technology (IT) Security</td>
</tr>
<tr>
<td>OVERSEE &amp; GOVERN</td>
<td>Strategize, Lead, Manage, Cybersecurity Systems &amp; Operations</td>
</tr>
<tr>
<td>PROTECT &amp; DEFEND</td>
<td>Identify, Analyze, Mitigate, Cybersecurity Threats</td>
</tr>
<tr>
<td>ANALYZE</td>
<td>Review, Evaluate, Cybersecurity Information</td>
</tr>
<tr>
<td>COLLECT &amp; OPERATE</td>
<td>Collect, Operate, Denial and Deception Operations</td>
</tr>
<tr>
<td>INVESTIGATE</td>
<td>Identify, Collect, Examine, IT systems &amp; Network Evidence</td>
</tr>
</tbody>
</table>
## SECURELY PROVISION

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

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>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 cybersecurity and risk requirements.</td>
<td>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.</td>
<td>Conducts technology assessment and integration processes; provides and supports a prototype capability and/or evaluates its utility.</td>
<td>Consults with customers to gather and evaluate functional requirements and translates these requirements into technical solutions. Provides guidance to customers about applicability of information systems to meet business needs.</td>
<td>Develops and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices.</td>
<td>Works on the development phases of the systems development life cycle.</td>
<td>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 systems or elements of systems incorporating IT.</td>
</tr>
</tbody>
</table>

### Roles:
- **Authorizing Official/Designating Representative**
- **Security Control Assessor**

### Our Solutions:
- **Certified Chief Information Security Officer**
- **CompTIA Security+**
- **CompTIA PenTest+**
- **CompTIA Cybersecurity Analyst (CySA+)**
- **CompTIA Advanced Security Practitioner (CASP+)**
- **CompTIA Cloud+**

- **Enterprise Architect**
- **Research & Development Specialist**

- **Certified Application Security Engineer (CASE Java)**
- **Certified Application Security Engineer (CASE .Net)**
- **CompTIA Cybersecurity Analyst (CySA+)**
- **CompTIA Cloud+**
- **CompTIA PenTest+**

- **Information Systems Security Developer**
- **Systems Developer**

- **System Testing and Evaluation Specialist**

- **Certified Network Defender V2 (CND)**
- **Certified Ethical Hacker V11 (CEH)**
- **CompTIA Advanced Security Practitioner (CASP+)**
- **CompTIA Cloud+**

- **Certified Network Defender V2 (CND)**
- **Certified Application Security Engineer (CASE Java)**
- **Certified Application Security Engineer (CASE .Net)**
- **CompTIA Cybersecurity Analyst (CySA+)**
- **CompTIA Cloud+**
- **CompTIA PenTest+**

- **Certified Network Defender V2 (CND)**
- **CompTIA Advanced Security Practitioner (CASP+)**
- **CompTIA Cybersecurity Analyst (CySA+)**
- **CompTIA Cloud+**
- **CompTIA PenTest+**
## OPERATE & MAINTAIN

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

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Administration (DTA)</td>
<td>Develops and administers databases and/or data management systems that allow for the storage, query, protection, and utilization of data.</td>
</tr>
<tr>
<td>Knowledge Management (KMG)</td>
<td>Manages and administers processes and tools that enable the organization to identify, document, and access intellectual capital and information content.</td>
</tr>
<tr>
<td>Customer Service and Technical Support (STS)</td>
<td>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.</td>
</tr>
<tr>
<td>Network Services (NET)</td>
<td>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.</td>
</tr>
<tr>
<td>Systems Administration (ADM)</td>
<td>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.</td>
</tr>
<tr>
<td>Systems Analysis (ANA)</td>
<td>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.</td>
</tr>
</tbody>
</table>

### Roles:
- Database Administrator
- Knowledge Manager
- Technical Support Specialist
- Network Operations Specialist
- System Administrator
- Systems Security Analyst

### Our Solutions:
- CompTIA Cybersecurity Analyst (CySA+)
- CompTIA Cloud+
- CompTIA PenTest+
- CompTIA Server+
- CompTIA A+
- CompTIA Network+
- CompTIA Security+
- CompTIA Cybersecurity Analyst (CySA+)
- Certified Network Defender V2 (CND)
- CompTIA A+
- CompTIA Network+
- CompTIA Security+
- CompTIA Cloud+
- CompTIA Server+
- Certified Network Defender V2 (CND)
- CompTIA A+
- CompTIA Network+
- CompTIA Security+
- CompTIA Cloud+
- CompTIA Server+
- Certified Network Defender V2 (CND)
- CompTIA A+
- CompTIA Network+
- CompTIA Security+
- CompTIA Cloud+
- CompTIA Server+
- Certified Network Defender V2 (CND)
- CompTIA A+
- CompTIA Network+
- CompTIA Security+
- CompTIA Cloud+
- CompTIA Server+
- Certified Network Defender V2 (CND)
- CompTIA A+
- CompTIA Network+
- CompTIA Security+
- CompTIA Cloud+
- CompTIA Server+
- Certified Network Defender V2 (CND)
- CompTIA A+
- CompTIA Network+
- CompTIA Security+
- CompTIA Cloud+
- CompTIA Server+
- Certified Network Defender V2 (CND)
- CompTIA A+
- CompTIA Network+
- CompTIA Security+
- CompTIA Cloud+
- CompTIA Server+
- Certified Network Defender V2 (CND)
- CompTIA A+
- CompTIA Network+
- CompTIA Security+
- CompTIA Cloud+
- CompTIA Server+
- Certified Network Defender V2 (CND)
- CompTIA A+
- CompTIA Network+
- CompTIA Security+
- CompTIA Cloud+
- CompTIA Server+
- Certified Network Defender V2 (CND)
- CompTIA A+
- CompTIA Network+
- CompTIA Security+
- CompTIA Cloud+
- CompTIA Server+
- Certified Network Defender V2 (CND)
- CompTIA A+
- CompTIA Network+
- CompTIA Security+
- CompTIA Cloud+
- CompTIA Server+
- Certified Network Defender V2 (CND)
- CompTIA A+
- CompTIA Network+
- CompTIA Security+
- CompTIA Cloud+
- CompTIA Server+
- Certified Network Defender V2 (CND)
- CompTIA A+
- CompTIA Network+
- CompTIA Security+
- CompTIA Cloud+
- CompTIA Server+
- Certified Network Defender V2 (CND)
- CompTIA A+
- CompTIA Network+
- CompTIA Security+
- CompTIA Cloud+
- CompTIA Server+
- Certified Network Defender V2 (CND)
- CompTIA A+
- CompTIA Network+
- CompTIA Security+
- CompTIA Cloud+
- CompTIA Server+
- Certified Network Defender V2 (CND)
- CompTIA A+
- CompTIA Network+
- CompTIA Security+
- CompTIA Cloud+
- CompTIA Server+
- Certified Network Defender V2 (CND)
- CompTIA A+
- CompTIA Network+
- CompTIA Security+
- CompTIA Cloud+
- CompTIA Server+
- Certified Network Defender V2 (CND)
- CompTIA A+
- CompTIA Network+
- CompTIA Security+
- CompTIA Cloud+
- CompTIA Server+
- Certified Network Defender V2 (CND)
- CompTIA A+
- CompTIA Network+
- CompTIA Security+
- CompTIA Cloud+
- CompTIA Server+
- Certified Network Defender V2 (CND)
- CompTIA A+
- CompTIA Network+
- CompTIA Security+
- CompTIA Cloud+
- CompTIA Server+
- Certified Network Defender V2 (CND)
- CompTIA A+
- CompTIA Network+
- CompTIA Security+
- CompTIA Cloud+
- CompTIA Server+
- Certified Network Defender V2 (CND)
- CompTIA A+
- CompTIA Network+
- CompTIA Security+
- CompTIA Cloud+
- CompTIA Server+
- Certified Network Defender V2 (CND)
- CompTIA A+
- CompTIA Network+
- CompTIA Security+
- CompTIA Cloud+
- CompTIA Server+
- Certified Network Defender V2 (CND)
- CompTIA A+
- CompTIA Network+
- CompTIA Security+
- CompTIA Cloud+
- CompTIA Server+
- Certified Network Defender V2 (CND)
- CompTIA A+
- CompTIA Network+
- CompTIA Security+
- CompTIA Cloud+
- CompTIA Server+
- Certified Network Defender V2 (CND)
- CompTIA A+
- CompTIA Network+
- CompTIA Security+
- CompTIA Cloud+
- CompTIA Server+
- Certified Network Defender V2 (CND)
- CompTIA A+
- CompTIA Network+
- CompTIA Security+
- CompTIA Cloud+
- CompTIA Server+
- Certified Network Defender V2 (CND)
- CompTIA A+
- CompTIA Network+
- CompTIA Security+
- CompTIA Cloud+
- CompTIA Server+
- Certified Network Defender V2 (CND)
- CompTIA A+
- CompTIA Network+
- CompTIA Security+
- CompTIA Cloud+
- CompTIA Server+
- Certified Network Defender V2 (CND)
- CompTIA A+
- CompTIA Network+
- CompTIA Security+
- CompTIA Cloud+
- CompTIA Server+
- Certified Network Defender V2 (CND)
- CompTIA A+
- CompTIA Network+
- CompTIA Security+
- CompTIA Cloud+
- CompTIA Server+
- Certified Network Defender V2 (CND)
- CompTIA A+
- CompTIA Network+
- CompTIA Security+
- CompTIA Cloud+
- CompTIA Server+
- Certified Network Defender V2 (CND)
- CompTIA A+
- CompTIA Network+
- CompTIA Security+
- CompTIA Cloud+
- CompTIA Server+
- Certified Network Defender V2 (CND)
- CompTIA A+
- CompTIA Network+
- CompTIA Security+
- CompTIA Cloud+
- CompTIA Server+
- Certified Network Defender V2 (CND)
- CompTIA A+
- CompTIA Network+
- CompTIA Security+
- CompTIA Cloud+
- CompTIA Server+
- Certified Network Defender V2 (CND)
- CompTIA A+...
## OVERSEE & GOVERN

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

<table>
<thead>
<tr>
<th>Legal Advice and Advocacy (LGA)</th>
<th>Training, Education, and Awareness (TEA)</th>
<th>Cybersecurity Management (MGT)</th>
<th>Strategic Planning and Policy (SPP)</th>
<th>Executive Cyber Leadership (EXL)</th>
<th>Program/Project Management (PMA) and Acquisition</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td>Conducts training of personnel within pertinent subject domain. Develops, plans, coordinates, delivers and/or evaluates training courses, methods, and techniques as appropriate.</td>
<td>Oversees the cybersecurity 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.</td>
<td>Develops policies and plans and/or advocates for changes in policy that support organizational cyberspace initiatives or required changes/enhancements.</td>
<td>Supervises, manages, and/or leads work and workers performing cyber and cyber-related and/or cyber operations work.</td>
<td>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.</td>
</tr>
</tbody>
</table>

### Roles:

- **Cyber Legal Advisor**
- **Privacy Officer/Privacy Compliance Manager**
- **Cyber Instructional Curriculum Developer**
- **Cyber Instructor**
- **Information Systems Security Manager**
- **Communications Security (COMSEC) Manager**
- **Cyber Workforce Developer and Manager**
- **Cyber Policy and Strategy Planner**
- **Executive Cyber Leadership**
- **Program Manager**
- **IT Project Manager**
- **Product Support Manager**
- **IT Investment/Portfolio Manager**
- **IT Program Auditor**

### Our Solutions:

- **CompTIA Cybersecurity Analyst (CySA+)**
- **CompTIA Cloud+**
- **Certified Network Defender V2 (CND)**
- **CompTIA Advanced Security Practitioner (CASP+)**
- **Certified Network Defender V2 (CND)**
- **CompTIA Advanced Security Practitioner (CASP+)**
- **Certified Network Defender V2 (CND)**
- **CompTIA Cloud+**
- **CompTIA Advanced Security Practitioner (CASP+)**
**PROTECT & DEFEND**

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

### Cybersecurity Defense Analysis (CDA)
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.

**Roles:**
- Cyber Legal Advisor
- Cyber Defense Infrastructure Support Specialist

**Our Solutions:**
- CompTIA Security+
- CompTIA Network+
- CompTIA PenTest+
- CompTIA Cybersecurity Analyst (CySA+)
- CompTIA Advanced Security Practitioner (CASP+)
- Certified Ethical Hacker V11 (CEH)
- CompTIA Cloud+
- Certified Network Defender V2 (CND)

### Cybersecurity Defense Infrastructure Support (INF)
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.

**Roles:**
- Cyber Defense Incident Responder

**Our Solutions:**
- CompTIA Security+
- CompTIA A+
- CompTIA Network+
- CompTIA PenTest+
- CompTIA Cybersecurity Analyst (CySA+)
- CompTIA Advanced Security Practitioner (CASP+)
- Certified Incident Handler (ECIH)

### Incident Response (CIR)
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.

**Roles:**
- Vulnerability Assessment Analyst

**Our Solutions:**
- CompTIA Security+
- CompTIA Network+
- CompTIA PenTest+
- CompTIA Cybersecurity Analyst (CySA+)
- CompTIA Advanced Security Practitioner (CASP+)
- Certified Incident Handler (ECIH)
- CompTIA Project+

### Vulnerability Assessment and Management (VAM)
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.
## Analyze

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

<table>
<thead>
<tr>
<th>Threat Analysis (TWA)</th>
<th>Exploitation Analysis (EXP)</th>
<th>All-Source Analysis (ASA)</th>
<th>Targets (TGT)</th>
<th>Language Analysis (LNG)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifies and assesses the capabilities and activities of cybersecurity criminals or foreign intelligence entities; produces findings to help initialize or support law enforcement and counter-intelligence investigations or activities. Performs highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.</td>
<td>Analyzes collected information to identify vulnerabilities and potential for exploitation.</td>
<td>Analyzes threat information from multiple sources, disciplines, and agencies across the Intelligence Community. Synthesizes and places intelligence information in context; draws insights about the possible implications.</td>
<td>Applies current knowledge of one or more regions, countries, non-state entities, and/or technologies.</td>
<td>Applies language, cultural, and technical expertise to support information collection, analysis, and other cybersecurity activities.</td>
</tr>
</tbody>
</table>

**Roles:**
- Cyber Legal Advisor

**Our Solutions:**
- CompTIA PenTest+  
- CompTIA Cybersecurity Analyst (CySA+)  
- CompTIA Advanced Security Practitioner (CASP+)
- Certified Ethical Hacker V11 (CEH)

**Roles:**
- Cyber Legal Advisor

**Our Solutions:**
- CompTIA PenTest+  
- CompTIA Cybersecurity Analyst (CySA+)

**Roles:**
- All-Source Analyst  
- Mission Assessment Specialist

**Our Solutions:**
- CompTIA Cloud+

**Roles:**
- Target Developer  
- Target Network Analyst

**Roles:**
- Multi-Disciplined Language Analyst
## COLLECT & OPERATE

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

<table>
<thead>
<tr>
<th>Threat Analysis (TWA)</th>
<th>Exploitation Analysis (EXP)</th>
<th>All-Source Analysis (ASA)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Roles:</strong> Cyber Legal Advisor</td>
<td><strong>Roles:</strong> Cyber Legal Advisor</td>
<td><strong>Roles:</strong> All-Source Analyst, Mission Assessment Specialist</td>
</tr>
<tr>
<td><strong>Our Solutions:</strong> CompTIA Cybersecurity Analyst (CySA+), CompTIA Advanced Security Practitioner (CASP+)</td>
<td><strong>Our Solutions:</strong> CompTIA Cybersecurity Analyst (CySA+), CompTIA Advanced Security Practitioner (CASP+), CompTIA PenTest+, CompTIA Project+</td>
<td><strong>Our Solutions:</strong> CompTIA Cybersecurity Analyst (CySA+), CompTIA Advanced Security Practitioner (CASP+), CompTIA PenTest+</td>
</tr>
</tbody>
</table>
INVESTIGATE

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

<table>
<thead>
<tr>
<th>Cyber Investigation (INV)</th>
<th>Digital Forensics (FOR)</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td>Collects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations.</td>
</tr>
</tbody>
</table>

**Roles :-**

- Cyber Legal Advisor

**Our Solutions :-**

- Computer Hacking Forensic Investigator V10
- CompTIA PenTest+

**Roles :-**

- Cyber Legal Advisor

**Our Solutions :-**

- Computer Hacking Forensic Investigator V10
- CompTIA PenTest+
- CompTIA Security+
- CompTIA Cybersecurity Analyst (CySA+)
- CompTIA Advanced Security Practitioner (CASP+)
- CompTIA Network+