Attachment H-1: Labor Category (LCAT) Descriptions

H.4.1 Overhead and DAWSON Segment LCAT Descriptions

CLIN 01-01 – Program Manager / Contract Delivery Manager
CLIN 01-02 – Program Manager / Contract Delivery Manager

The Program Manager is responsible for the full lifecycle execution of the contract and its four technical segments (Cybersecurity, DAWSON, Strategic Initiatives, Help Desk)

The Program Manager serves as the primary contractual contact for ensuring successful execution of the contract including performance tracking across all segments and CLINs, and communicating resource allocation and utilization, workforce management, financial compliance, and negotiating contract modifications. This role requires significant experience in large-scale contract management, financial oversight, and technical program leadership.

Key Responsibilities

- Program Oversight & Execution: Lead the successful execution of all contract requirements, ensuring alignment with financial, operational, and performance metrics.
- Financial & FTE Tracking: Oversee and report on FTE utilization, ensuring that actual labor hours executed align with the number of paid FTEs for each period. Provide financial tracking of labor costs and invoice reconciliation.
- Cost Reporting & Compliance: Ensure financial reporting is structured to support the Court financial accounting requirements such as detailing labor hours for capitalization, and cost variances against contract budget.
- Contract Management: Manage the negotiation and execution of additional CLINs, project pricing, and modifications to the existing contract including defining and reporting Key Performance Indicators (KPIs) for staff augmentation and project-based work.
- Personnel Management: Resolve staffing issues, manage the allocation of personnel across technical segments, and ensure workforce satisfaction and retention.
- Stakeholder Communication: Serve as the primary liaison between internal teams, customer stakeholders, and the Court's IT leadership, ensuring all parties are informed of program status and performance.
- Risk & Issue Management: Identify potential risks related to staffing, project timelines, and contractual obligations, and proactively implement mitigation strategies.
- Quality Control & Compliance: Ensure the contract's deliverables meet both technical specifications and security compliance for the Court's systems and operations.

Skills and Qualifications:

- Program Management: Expertise in managing large-scale IT contracts with a focus on staff augmentation, including the ability to oversee multi-domain technical teams.
- Financial Management: Strong knowledge of budgeting, financial reporting, and labor hour tracking for contracts involving FTEs and multi-year funding.
- Contractual Negotiation: Extensive experience negotiating CLIN modifications, project pricing, and contract adjustments within a government contracting environment.
- Personnel & Resource Coordination: Demonstrated ability to manage and resolve personnel issues in diverse technical domains, ensuring efficient staffing and resource utilization.
- Government Contracting: In-depth understanding of federal contracting procedures, including compliance with FAR and agency-specific requirements.
- Technical Knowledge: Familiarity with cybersecurity best practices, IT service management (ITSM), and physical security systems (e.g., PACs and video surveillance).

Certifications:

- Project Management: PMP (Project Management Professional)
- Program Management: PgMP (Program Management Professional)
- Portfolio Management: PfMP (Portfolio Management Professional)
- IT Service Management: ITIL v4
- Government Contracting: DAWIA Level III
- Agile Practices: Scaled Agile Framework (SAFe), Agile Business Process Management Specialist.

Required Experience:

- Project Management: A minimum of 8 years of experience in project management, focusing on large-scale contracts and staff augmentation models with government clients, ensuring alignment between resources, performance, and contract specifications.
- Program Management: A minimum of 5 years of experience in program management, overseeing multi-year projects involving diverse technical functions (e.g., cybersecurity, IT support, strategic initiatives, and security systems).
- Staff Augmentation & Contract Management: A minimum of 5 years of experience in managing contracts that require staff augmentation, resource coordination, and CLIN-based contract execution.
- Government Contracting: A minimum of 3 years experience working with federal contracts, specifically in the areas of CLIN management, modifications, and budget oversight.

CLIN 02-01 – DevOps Engineer
CLIN 02-09 – DevOps Engineer

Backend engineer with specialty of ensuring application deployment, automated continuous integration testing, and ensuring visibility of performance and key metrics to inform developers' decision making.

- **Communication and Collaboration**: have effective communication skills and the ability to collaborate within a team environment, including sharing progress, asking for help when needed, and providing constructive feedback.
- **Continuous Learning**: have an eagerness to learn and adapt to new technologies, frameworks, and best practices in web development and cloud infrastructure management.
- **Technology Knowledge**: maintain knowledge and skills on existing and emerging agile best practices, technologies relevant to supported projects, security best practices, etc.
- **Skills & Qualifications:**
    - Version Control: with version control systems like Git for collaborative development and managing codebase changes.
    - Terraform: Basic understanding of Infrastructure as Code (IaC) principles and experience with Terraform for provisioning and managing infrastructure resources on cloud platforms such as AWS, Azure, or Google Cloud Platform.
    - **CI/CD Pipelines:** GitHub Actions, CircleCI, GitLab CI/CD, ArgoCD, Jenkins.
    - **Scripting & Automation** – Python, Bash, Go, PowerShell.
    - **Linux & System Administration** – File systems, process management, performance tuning.
    - AWS Services: Familiarity with core AWS services such as:
        - AWS Lambda for serverless functions
        - AWS S3 for storage
        - AWS API Gateway for creating RESTful APIs
        - AWS DynamoDB for NoSQL database
        - AWS EC2 for virtual servers
        - AWS RDS for managed relational databases
        - AWS CloudFront for content delivery
        - AWS CloudWatch for Application Monitoring
    - **Database Management** – PostgreSQL, MySQL, MongoDB, Redis.
- **Education:** Bachelor's in computer science or equivalent work experience
- **Certification:**
    - AWS Certified DevOps Engineer
- **Required Experience:**
    - 5 years of experience working with AWS, infrastructure as code (Terraform, CloudFormation, etc.), CI/CD pipelines (GitHub Actions, CircleCI, etc.), containerization (Docker, Kubernetes, etc.), and scripting (Python, Bash, etc.).
    - 3 years of experience working with TypeScript/JavaScript.

CLIN 02-02 – Delivery Manager
CLIN 02-10 – Delivery Manager

Managing team resources, identifying blockers and tackled, and ensuring delivery of solutions.

- **Communication and Collaboration**: have effective communication skills and the ability to collaborate within a team environment, including sharing progress, asking for help when needed, and providing constructive feedback.
- **Technology Knowledge**: maintain knowledge and skills on existing and emerging agile best practices, technologies relevant to supported projects, security best practices, etc.
- **Skills & Qualifications**
    - **Project Management:** Agile (Scrum, Kanban, SAFe), Github Issues, Monday.com, Jira
    - **Delivery Planning:** Roadmap creation, sprint planning, backlog prioritization.
    - **Stakeholder Management:** Communication with executives, customers, and tech teams.
    - **Risk & Issue Management:** Identifying bottlenecks and mitigating risks proactively.
    - **Process Optimization:** Continuous improvement using retrospectives, OKRs, and KPIs.
    - **Budgeting & Resource Allocation:** Managing costs and team capacity.
    - **Technical Awareness:** Understanding software development, DevOps, cloud, and CI/CD (not hands-on but enough to communicate effectively with engineers).
- **Education:**
    - Bachelor's or equivalent work experience
- **Required Experience:**
    - Minimum of 6 years of experience managing teams of developers, working with stakeholders, and delivering software projects using Agile methodologies.

CLIN 02-03 – Senior Web Developer
CLIN 02-11 – Senior Web Developer

Full-Stack Developer with expertise in TypeScript, Node.js, React.js, Terraform, CSS, and AWS Services.

- **Communication and Collaboration**: have effective communication skills and the ability to collaborate within a team environment, including sharing progress, asking for help when needed, and providing constructive feedback.
- **Continuous Learning**: have an eagerness to learn and adapt to new technologies, frameworks, and best practices in web development and cloud infrastructure management.
- **Technology Knowledge**: maintain knowledge and skills on existing and emerging agile best practices, technologies relevant to supported projects, security best practices, etc.

- **Skills & Qualifications:**
    - JavaScript/TypeScript: Experience and proficiency in JavaScript and/or TypeScript.
    - React.js: Working knowledge of React.js library for building user interfaces and Single Page Applications (SPAs).
    - HTML/CSS: Mastery of HTML and CSS for structuring and styling web pages.
    - Node.js: Proficiency with Node.js for building server-side applications and handling dependencies with tools like npm or yarn.
    - Python/pytest: Experience with Python for building packages and solutions as well as writing unit tests and integration tests.
    - Version Control: Experience with version control systems like Git for collaborative development and managing codebase changes.
    - Terraform: Basic understanding of Infrastructure as Code (IaC) principles and experience with Terraform for provisioning and managing infrastructure resources on cloud platforms such as AWS, Azure, or Google Cloud Platform.
    - AWS Services: Familiarity with core AWS services such as:
        - AWS Lambda for serverless functions
        - AWS S3 for storage
        - AWS API Gateway for creating RESTful APIs
        - AWS DynamoDB for NoSQL database
        - AWS EC2 for virtual servers
        - AWS RDS for managed relational databases
        - AWS CloudFront for content delivery
        - AWS CloudWatch for Application Monitoring
    - Microsoft Azure / Office 365:
        - SharePoint for file, web part, and list management
    - API Integration: Ability to integrate RESTful APIs endpoints with the React frontend to fetch and manipulate data.
    - Debugging and Testing: Proficiency in debugging React applications and writing unit tests using libraries like Jest and React Testing Library.
- **Education:**
    - Bachelor's or equivalent work experience
- **Certifications:**
    - AWS Certified Solutions Architect Associate
- **Required Experience:**
    - Minimum of 6 years of experience working with TypeScript/JavaScript, CSS, SASS, HTML, Node.js, Github, and React.js (or other JavaScript frameworks).
    - 4 years of experience working with AWS, infrastructure as code (Terraform, CloudFormation), CI/CD pipelines (GitHub Actions, CircleCI, etc.), containerization (Docker, Kubernetes, etc.), and scripting (Python, Bash, etc.).

CLIN 02-04 – Systems Engineer
CLIN 02-12 – Systems Engineer

Full-Stack Developer with expertise in AWS Services, Terraform, TypeScript, and ensuring visibility of performance and key metrics to inform developers' decision making.

- **Communication and Collaboration**: have effective communication skills and the ability to collaborate within a team environment, including sharing progress, asking for help when needed, and providing constructive feedback.
- **Continuous Learning**: have an eagerness to learn and adapt to new technologies, frameworks, and best practices in web development and cloud infrastructure management.
- **Technology Knowledge**: maintain knowledge and skills on existing and emerging agile best practices, technologies relevant to supported projects, security best practices, etc.
- **Skills & Qualifications:**
    - Version Control: Experience with version control systems like Git for collaborative development and managing codebase changes.
    - Terraform: Basic understanding of Infrastructure as Code (IaC) principles and experience with Terraform for provisioning and managing infrastructure resources on cloud platforms such as AWS, Azure, or Google Cloud Platform.
    - **CI/CD Pipelines:** GitHub Actions, CircleCI, GitLab CI/CD, ArgoCD, Jenkins.
    - **Scripting & Automation** – Python, Bash, Go, PowerShell.
    - **Linux & System Administration** – File systems, process management, performance tuning.
    - AWS Services: Familiarity with core AWS services such as:
        - AWS Lambda for serverless functions
        - AWS S3 for storage
        - AWS API Gateway for creating RESTful APIs
        - AWS DynamoDB for NoSQL database
        - AWS EC2 for virtual servers
        - AWS RDS for managed relational databases
        - AWS CloudFront for content delivery
        - AWS CloudWatch for Application Monitoring
    - **Database Management** – PostgreSQL, MySQL, MongoDB, Redis.
- **Education:** Bachelor's in computer science or equivalent work experience
- **Certifications:**
    - AWS Certified Solutions Architect Associate
- **Required Experience:**
    - Minimum of 4 years of experience working with TypeScript/JavaScript, CSS, SASS, HTML, Node.js, Github, and React.js (or other JavaScript frameworks).
    - Minimum of 6 years of experience working with AWS, infrastructure as code (Terraform, CloudFormation, etc.), CI/CD pipelines (GitHub Actions, CircleCI,

etc.), containerization (Docker, Kubernetes, etc.), and scripting (Python, Bash, etc.).

CLIN 02-05 – UX Researcher / Designer
CLIN 02-13 – UX Researcher / Designer

User Experience and mobile/desktop design experience with an emphasis on accessibility/usability testing.

- **Communication and Collaboration**: have effective communication skills and the ability to collaborate within a team environment, including sharing progress, asking for help when needed, and providing constructive feedback.
- **Continuous Learning**: have an eagerness to learn and adapt to new technologies, frameworks, and best practices in web development.
- **Skills & Qualifications**:
    - User Research: ability to conduct and analyze user research, interviews, and surveys.
    - Wireframing and Prototyping: creating basic blueprints of design layouts and interactive prototypes in tools like Figma, Sketch, Adobe XD, etc.
    - Visual Design: Knowledge of font choices, color schemes, and how they impact user experience as well as an understanding of grid systems, balance, and visual hierarchy.
    - Interactive Design: designing smooth transitions, animations, and feedback loops as well as designs that work well across different devices and screen sizes.
    - Information Architecture: structuring information in a way that is logical and easy to navigate and creating intuitive navigation systems.
    - Design Tools: Proficiency in tools like Figma, Sketch, Adobe Creative Suite as well as basic HTML/CSS knowledge.
    - Usability Testing: Planning and conducting tests to validate design decisions and the ability to refine designs based on feedback and test results.
    - Problem-Solving and Critical Thinking: Approaching design challenges with the user's needs in mind and taking an iterative approach towards refining designs and ideas.
    - Attention to Detail: Ensuring every element is perfectly aligned and visually consistent, and the design language is consistent throughout the product or suite of products.
- **Education:**
    - Bachelor's or equivalent work experience
- **Required Experience:**
    - Minimum of 4 years of experience with user research, wireframing, prototyping, and visual design.
    - Minimum of 4 years of experience using design tools such as Figma, Sketch, or Adobe XD

- Minimum of 4 years of experience using design systems, usability principles, and accessibility standards (WCAG).
- Minimum of 4 years of experience on software projects that involved conducting user interviews, surveys, A/B testing, and heuristic evaluations to drive design decisions.

CLIN 02-06 – Web Developer
CLIN 02-14 – Web Developer

Full-Stack Developer with limited experience in TypeScript, Node.js, React.js, CSS, SASS, and AWS Services.

- **Communication and Collaboration**: have effective communication skills and the ability to collaborate within a team environment, including sharing progress, asking for help when needed, and providing constructive feedback.
- **Continuous Learning**: have an eagerness to learn and adapt to new technologies, frameworks, and best practices in web development.
- **Technology Knowledge**: maintain knowledge and skills on existing and emerging agile best practices, technologies relevant to supported projects, security best practices, etc.
- Skills & Qualifications:
  - **JavaScript/TypeScript**: Experience and proficiency in JavaScript and/or TypeScript.
  - **React.js:** Working knowledge of React.js library for building user interfaces and Single Page Applications (SPAs).
  - **Next.**js: Working knowledge of Next.js library for building web applications with React.js and Node.js.
  - **HTML/CSS**: Working knowledge of HTML and CSS for structuring and styling web pages.
  - **Node.js:** Familiarity with Node.js for building server-side applications and handling dependencies with tools like npm or yarn.
  - **Version Control**: Experience with version control systems like Git for collaborative development and managing codebase changes.
  - **AWS Services**: Familiarity with core AWS services such as:
    - **AWS Lambda** for serverless functions
    - **AWS S3** for storage
    - **AWS API Gateway** for creating RESTful APIs
    - **AWS DynamoDB** for NoSQL database
    - **AWS EC2** for virtual servers
    - **AWS RDS** for managed relational databases
    - **AWS CloudFront** for content delivery
  - **API Integration:** Ability to integrate RESTful APIs endpoints with the React frontend to fetch and manipulate data.
  - **Debugging and Testing:** Proficiency in debugging React applications and writing unit tests using libraries like Jest and React Testing Library.
- **Education:**

- Bachelor's or equivalent work experience
- **Required Experience:**
  - 2 years of experience working with TypeScript/JavaScript, CSS, SASS, HTML, Node.js, Github, and React.js (or other JavaScript frameworks).
  - 1 year of experience working with AWS, infrastructure as code (Terraform, CloudFormation, etc.), CI/CD pipelines (GitHub Actions, CircleCI, etc.), containerization (Docker, Kubernetes, etc.), and scripting (Python, Bash, etc.).

CLIN 02-07 -- Software Quality Assurance Engineer
CLIN 02-15 -- Software Quality Assurance Engineer

Responding to user support requests and feedback, researching user needs, setting and maintaining quality standards by QA testing, and developing product training materials.

- **Communication and Collaboration**: have effective communication skills and the ability to collaborate within a team environment, including sharing progress, asking for help when needed, and providing constructive feedback.
- **Continuous Learning**: have an eagerness to learn and adapt to new technologies, frameworks, and best practices in web development and cloud infrastructure management.
- **Technology Knowledge**: maintain knowledge and skills on existing and emerging agile best practices, technologies relevant to supported projects, security best practices, etc.
- **Skills & Qualifications**:
  - **Software Testing:** Strong knowledge of manual and automated testing methodologies.
  - **Automation Tools:** Experience with testing frameworks like **Selenium, Cypress, or Playwright.**
  - **Programming Knowledge:** Experience with **Python, JavaScript, or C#** for test automation scripting.
  - **Test Management Tools:** Familiarity with tools like **JIRA, TestRail, or Zephyr** for test case management.
  - **API Testing:** Experience using **Postman, REST Assured, or SoapUI** for API testing.
  - **Performance Testing:** Understanding of tools like **Artillery, JMeter, Gatling, or LoadRunner** to test application scalability and speed.
  - **CI/CD Pipelines:** Experience integrating tests into **CI/CD workflows** using Jenkins, GitHub Actions, CircleCI, or GitLab CI.
- **Education:**
  - Bachelor's or equivalent work experience
- **Required Experience:**
  - 4 years of experience with software testing, including manual and automated testing, testing tools like Selenium, Cypress, or Playwright for automation,

along with experience in API testing using tools like Postman or Jmeter, and test case tools like TestRails.

CLIN 02-08 – Web Designer

Graphic designer with a solid understanding of visual design principles, user experience (UX), and modern web technologies, responsible for designing aesthetically appealing and functional websites, web components, and user interfaces.

- **Communication and Collaboration**: have effective communication skills and the ability to collaborate within a team environment, including sharing progress, asking for help when needed, and providing constructive feedback.
- **Continuous Learning**: have an eagerness to learn and adapt to new technologies, frameworks, and best practices in web development.
- **Technology Knowledge**: maintain knowledge and skills on existing and emerging agile best practices, technologies relevant to supported projects, security best practices, etc.
- **Skills & Qualifications:**
    - Wireframing and Prototyping: creating basic blueprints of design layouts and interactive prototypes in tools like Figma, Sketch, Adobe XD, etc.
    - Visual Design: Knowledge of font choices, color schemes, and how they impact user experience as well as an understanding of grid systems, balance, and visual hierarchy.
    - Interactive Design: designing smooth transitions, animations, and feedback loops as well as designs that work well across different devices and screen sizes.
    - Information Architecture: structuring information in a way that is logical and easy to navigate and creating intuitive navigation systems.
    - Design Tools: Proficiency in tools like Figma, Sketch, Adobe Creative Suite as well as basic HTML/CSS knowledge.
    - Problem-Solving and Critical Thinking: Approaching design challenges with the user's needs in mind and taking an iterative approach towards refining designs and ideas.
    - Attention to Detail: Ensuring every element is perfectly aligned and visually consistent, and the design language is consistent throughout the product or suite of products.
- **Education:**
    - Bachelor's or equivalent work experience
- **Required Experience:**
    - Minimum of 4 years of experience with visual design, UI/UX principles, and responsive web design.
    - Minimum of 4 years of experience using tools like Figma, Adobe XD, or Sketch.
    - Minimum of 4 years of experience with design systems, typography, color theory, and accessibility standards (WCAG).
    - Minimum of 2 years of experience with basic HTML and CSS.

H.4.2 Help Desk Segment LCAT Descriptions

CLIN 03-01 – Senior Help Desk Technician
CLIN 03-05 – Senior Help Desk Technician

Provide high-level technical support and troubleshooting assistance for end-users across a broad range of IT systems and applications. The Senior Help Desk Technician will act as a subject matter expert (SME) for the IT support team, assisting with the resolution of complex technical issues, providing guidance and training to junior technicians, and ensuring effective solutions are implemented. Answer questions or resolve computer problems for clients in person, via telephone, or electronically. Will help when it comes to the use of computer hardware and software, including printing, installation, word processing, electronic mail, and operating systems.

Technical Support & Troubleshooting:

- Provide advanced technical support for end-users, resolving issues related to M365/O365 applications, Azure AD/Entra, Intune/Endpoint Manager, SharePoint, and VoIP (Poly Phones).
- Troubleshoot hardware and software issues related to both Mac and Windows laptops, iOS/Android mobile devices, and associated cloud services.
- Conduct root cause analysis to identify, resolve, and prevent recurring technical issues across multiple platforms, including network connectivity, hardware failures, and software compatibility.

Customer Service & User Support:

- Deliver high-quality customer service, ensuring users receive timely, efficient, and professional support.
- Provide clear communication and regular updates to end-users on issue status, working to resolve user problems in a courteous and timely manner.
- Demonstrate empathy and patience, especially in complex or stressful situations.
- Conduct training sessions for users on best practices for using Microsoft Office, SharePoint, Zoom, and mobile device management systems.

System Administration & Maintenance:

- Support and maintain the operation of cloud-based systems like M365/O365 and Azure AD, including account management, permissions, and security configurations.
- Manage mobile device configurations through Intune/Endpoint Manager and ensure compliance with security policies across all devices (Mac, Windows, mobile phones).
- Provide user access management in Azure AD and support collaboration platforms such as SharePoint, ensuring data security and collaboration.

Documentation & Reporting

- Maintain accurate and thorough records of support tickets, troubleshooting steps, resolutions, and service requests in Zendesk.
- Produce documentation and knowledge base articles to assist in future troubleshooting and ensure knowledge continuity.

Security & Compliance

- Support organizational cybersecurity efforts by ensuring devices, applications, and cloud services are compliant with security protocols, industry regulations, and internal policies.
- Provide guidance on security best practices, including password management, multi-factor authentication (MFA), and endpoint protection.

Skills & Qualifications:

Technical Skills

- Proficient in managing and troubleshooting M365/O365 applications, Azure AD/Entra, Intune/Endpoint Manager, SharePoint, and associated cloud-based services.
- Strong understanding of MacOS, Windows OS, iOS, and Android device management and troubleshooting.
- Experience with VoIP systems (Poly Phones, etc.) and related telecommunication technologies.
- Proficiency in troubleshooting hardware and software for both laptops (Mac and Windows) and mobile devices (iOS and Android).
- Knowledge of security camera systems (Axis Security Cameras) and related configurations.
- Familiarity with faxing solutions (Documo mFax) and Zoom communication platform.

Troubleshooting & Root Cause Analysis

- Strong diagnostic skills for identifying and resolving issues at the system, application, and user levels.
- Ability to perform root cause analysis to prevent recurring issues and recommend long-term solutions.

Customer Service & Communication Skills

- Excellent communication skills to effectively interact with end-users of various technical backgrounds.
- Strong customer service orientation with the ability to handle challenging customer situations in a professional and calm manner.
- Experience in providing training and technical support in an easy-to-understand, user-friendly manner.

Certifications:

Technical Certifications *

- Microsoft Certified: Azure Fundamentals or Microsoft Certified: Security, Compliance, and Identity Fundamentals
- CompTIA A+

- CompTIA Network+
- Microsoft Certified: Modern Desktop Administrator Associate
- Certified Information Systems Security Professional (CISSP) – for advanced security knowledge
- ITIL Foundation Certification for service management best practices
- Apple Certified Support Professional (ACSP) – for MacOS support proficiency

**Agreement to recertify within 3 months of start date if certifications have lapsed*

Customer Service Certifications

- HDI Support Center Analyst Certification
- ITIL Foundation for IT service management
- Microsoft Certified: Dynamics 365 Fundamentals (Customer Service)

Required Experience:

- Minimum of 8 years of experience in a technical support or IT help desk environment with progressive responsibility.
- At least 2 years of experience administering M365/O365, Azure AD/Entra, Intune/Endpoint Manager, SharePoint, and software-as-a-service solutions (e.g., Zoom, mFax, Teams, Eagle Eye, Brivo, Everbridge, or other cloud-based services).
- Proven experience supporting a diverse range of devices, including MacOS, Windows, mobile devices (iOS and Android), and cloud-based technologies.
- Solid background in troubleshooting complex IT problems and performing root cause analysis.
- Strong customer service experience with a focus on providing exceptional support in a fast-paced, multi-tasking environment.
- Previous experience working with ticketing systems, preferably Zendesk, and keeping accurate records of technical issues and resolutions.

Desirable Skills:

- Experience with telecommunication systems (VoIP like Poly Phones) and security camera systems (Axis, Eagle Eye).
- Knowledge of managing software as a service such as virtual faxing using Documo mFax, Everbridge, or Zoom/ZoomGov
- Experience working in a hybrid work environment supporting remote and on-site users.

CLIN 03-02 - Senior Help Desk Engineer
CLIN 03-08 - Senior Help Desk Engineer

Provide advanced technical support and ensures the effective operation of a wide range of IT systems and services within a dynamic, fast-paced environment. This role is critical in supporting end-users across various platforms, resolving complex technical issues, and maintaining seamless IT operations. The Senior Help Desk Engineer will be responsible for troubleshooting, managing, and optimizing a diverse suite of technologies including

M365/O365, Azure AD/Entra, Zendesk, Intune/Endpoint Manager, SharePoint, Microsoft Office, Mac and Windows laptops, iOS and Android smartphones, documo mFax, Zoom, Axis and Eagle Eye security cameras, VoIP (Poly Phones), and associated cloud services. Candidates will be expected to demonstrate a combination of advanced technical expertise, strong customer service skills, and the ability to troubleshoot and resolve a wide range of IT issues effectively.

Technical Support & Troubleshooting:

- Provide expert-level technical support to end-users for a variety of systems and devices, including M365/O365 applications, Azure AD/Entra, Intune/Endpoint Manager, SharePoint, VoIP phones, mobile devices (iOS/Android), security camera systems (Axis, Eagle Eye), and cloud-based technologies.
- Diagnose and resolve issues related to hardware and software, including operating system (Windows, macOS), network connectivity, and application issues.
- Perform root cause analysis to determine underlying issues and implement permanent fixes to prevent recurring problems.
- Manage and troubleshoot cloud-based environments, especially focusing on M365/O365, Azure AD/Entra, and associated services.
- Support and administer endpoint management solutions via Intune/Endpoint Manager for managing device configurations, security policies, and software updates.

Customer Service & User Support:

- Function as a primary point of contact for end-users and demonstrate a customer-first mindset, ensuring timely and professional resolution of technical issues.
- Communicate effectively with users to gather necessary information, set expectations, and provide clear status updates during issue resolution.
- Document and track all service requests and incidents using Zendesk or other ticketing systems, ensuring accurate and up-to-date records.
- Provide training and guidance to users on the proper use of hardware and software tools.
- Deliver a positive user experience by responding to requests promptly and empathetically while maintaining a high standard of professionalism

System Administration & Maintenance:

- Assist with routine system maintenance tasks, including patch management, updates, and configuration changes for both on-premises and cloud-based services.
- Monitor system performance and proactively address any issues that may arise, ensuring minimal disruption to end-users.
- Configure and maintain user accounts, permissions, and security settings across various systems, ensuring compliance with organizational policies and best practices.

Documentation & Reporting

- Create and maintain internal knowledge bases, troubleshooting guides, and system configurations.

- Generate regular reports on system performance, issue resolution metrics, and support ticket trends.
- Strong documentation and reporting practices will also support audit trails, enhance communication within teams, and facilitate training and onboarding of new staff members.

Security & Compliance

- Tasked with monitoring and maintaining the security of user accounts, devices, and data through rigorous compliance with organizational policies and industry standards.
- Implements security measures such as multi-factor authentication, data encryption, and vulnerability patching.

Skills & Qualifications:

Technical Skills

- Strong knowledge of Microsoft 365/O365 services and applications (Word, Excel, Outlook, OneDrive, Teams, SharePoint, etc.).
- Advanced experience with Azure AD/Entra, including user and group management, authentication, security policies, and directory synchronization.
- Expertise in mobile device management via Intune/Endpoint Manager as well as configuration of mobile apps and policies (e.g., Endpoint Manager Apple Business Manager, Managed Google Play).
- Experience with cloud-based collaboration tools like Teams, Zendesk, and Zoom to understand how they integrate within an IT environment.
- Proficient with managing and troubleshooting Windows, macOS, iOS, and Android devices.
- Knowledge of network security best practices and familiarity with securing VoIP systems (Poly Phones) and surveillance camera systems (Axis, Eagle Eye).
- Familiarity with fax management systems like Documo mFax.
- Troubleshooting skills for a wide range of hardware and software issues across different platforms (PCs, laptops, mobile devices, etc.).
- Ability to diagnose and resolve complex networking issues (Wi-Fi, VPN, etc.).
- Experience with ticketing systems (Zendesk, ServiceNow, etc.) and incident management.
- Familiarity with security protocols, user authentication, and data encryption practices.
- Ability to mentor and provide guidance to junior help desk staff.
- Ability to manage multiple priorities and projects simultaneously while maintaining focus on customer satisfaction.
- Willingness to stay current with emerging technologies and best practices in the IT industry.

Customer Service & Communication Skills:

- Strong interpersonal communication skills to collaborate effectively with end-users of varying technical expertise.

- Excellent problem-solving abilities with a focus on delivering quality solutions to end-users in a timely manner.
- Ability to manage high-pressure situations while maintaining professionalism and customer satisfaction.
- Strong documentation skills for recording support requests, incidents, and resolutions.

Certifications:

Technical Certifications*

- Microsoft Certified: Azure Fundamentals, Microsoft Certified: Modern Desktop Administrator Associate, or Microsoft Certified: Security, Compliance, and Identity Fundamentals.
- CompTIA A+ or Network+ (for foundational IT knowledge and troubleshooting).
- Certified Information Systems Security Professional (CISSP) for a strong understanding of security practices.
- Apple Certified Support Professional (ACSP) for troubleshooting macOS- related issues.
- ITIL Foundation Certification for a standardized approach to IT service management.

** Agreement to recertify within 3 months of start date if certifications have lapsed*

Customer Service Certifications:

- HDI Support Center Analyst or HDI Desktop Support Technician for expertise in service desk operations and customer interaction.
- CompTIA IT Customer Service Specialist for customer service-oriented technical support roles.

Required Experience:

- Minimum of 8 years of hands-on experience in IT support or help desk roles, with a minimum 2 years in a senior-level position handling complex technical issues, especially periods working independently to achieve engineering outcomes.
- Extensive experience working with the PowerShell, tools and technologies mentioned above, including clous solutions related to M365/O365, Azure AD/Entra, Intune/Endpoint Manager, SharePoint, Printing, or VoIP systems.
- Proven history of providing high-quality customer service, both technical and non-technical, in a fast-paced environment.
- Experience working in a cloud-based environment and managing SaaS applications.
- Strong troubleshooting and root cause analysis skills, with the ability to independently resolve both technical and customer-related issues.

Desirable Skills:

- Extensive experience in managing M365/O365 environments, including Exchange Online, Teams, OneDrive, SharePoint, and Outlook.

- Deep understanding of Azure AD/Entra for user authentication, identity management, and access control. Expertise in configuring and maintaining SSO, MFA, and conditional access policies.
- Proficiency in deploying, securing, and managing Windows, macOS, iOS, and Android devices through Intune/Endpoint Manager, ensuring seamless integration and compliance with organizational policies.

CLIN 03-03 - Senior System Administrator
CLIN 03-11 - Senior System Administrator

Provides technical support, managing system maintenance, and troubleshooting a wide array of devices and software platforms. This role requires an individual who thrives in a fast-paced environment and has a passion for providing exceptional customer service while managing and securing a broad range of enterprise systems and services.

Technical Support & Troubleshooting:

- Provide expert-level support for both hardware and software issues across various devices, including Mac and Windows laptops, smartphones (iOS and Android), security cameras, VoIP systems, and associated cloud services.
- Troubleshoot and resolve issues related to M365/O365, Azure AD/Entra, SharePoint, Intune/Endpoint Manager, Zendesk, Documo mFax, Zoom, Axis and Eagle Eye security cameras, Poly Phones, and more.
- Perform root cause analysis of recurring technical issues and recommend long-term solutions.
- Act as the primary point of contact for complex technical problems, escalations, and incidents.

Customer Service & User Support:

- Communicate effectively with internal teams, stakeholders, and end-users to provide clear guidance and resolution to technical issues.
- Offer proactive customer service by identifying potential system improvements, upgrades, or changes that would benefit users and the Court.
- Train and support junior technicians and end-users to foster an environment of technical empowerment.

System Administration & Maintenance:

- Regularly monitor and maintain IT systems and services, ensuring they are up-to-date, secure, and optimized for performance.
- Perform system backups, updates, patch management, and ensure the ongoing integrity of IT environments.
- Manage and maintain Microsoft 365 environments, Azure AD/Entra, and associated services.
- Ensure endpoint devices (Windows, Mac, smartphones) are properly configured and compliant with organizational security policies using tools like Intune/Endpoint Manager.

Documentation & Reporting

- Develop, update, and maintain clear documentation for systems, processes, procedures, and troubleshooting steps.
- Provide knowledge sharing sessions and training materials to enhance the team's technical capabilities.
- Document service requests, incidents, and resolutions in a timely and accurate manner using Zendesk or equivalent ticketing systems.

Security & Compliance

- Ensures full compliance with internal security policies, industry standards, and applicable regulations.
- Deep understanding of system administration, security frameworks, and compliance requirements to safeguard systems and data against unauthorized access, breaches, and other security threats.

Skills & Qualifications:

Technical Skills

- Operating Systems: Expertise in supporting Windows and macOS, with a focus on device management, software deployment, and troubleshooting.
- Cloud Platforms: Hands-on experience with Microsoft 365/O365, Azure AD/Entra, SharePoint, and related cloud services.
- Device Management: Proficiency in Intune/Endpoint Manager for managing mobile and desktop devices, including policy enforcement, configuration management, and security management.
- Security & Compliance: Knowledge of security best practices, including encryption, MFA (Multi-Factor Authentication), and endpoint security solutions.
- Networking & Telephony: Familiarity with VoIP systems such as Poly Phones, networking infrastructure, and IP-based communications.
- Collaboration & Communication Tools: Experience with Zoom, Microsoft Teams, SharePoint, and other collaboration tools.
- Other Systems: Support and troubleshooting experience with Axis and Eagle Eye security cameras, Documo mFax, and various other IT systems.

Certifications:

Technical Certifications

- Microsoft Certified: Azure Administrator Associate or higher
- Microsoft Certified: Modern Desktop Administrator Associate
- CompTIA A+ (or equivalent experience)
- ITIL Foundation (desirable)
- Microsoft Certified: Security, Compliance, and Identity Fundamentals
- Microsoft Certified: M365 Certified: Enterprise Administrator Expert
- CompTIA Network+ or equivalent
- Certified Information Systems Security Professional (CISSP) or Certified Information Security Manager (CISM)
- Apple Certified Support Professional (ACSP) or Apple Certified Mac Technician (ACMT)
- VMware Certified Professional (VCP) for virtualization experience
- VoIP or Telephony-specific certifications (Polycom, Cisco, etc.)

Required Experience:

- Minimum of 8 years of experience as a Systems Administrator, IT Technician, or a similar role, supporting enterprise-level IT environments.
- Proven experience managing Microsoft 365/O365 environments, Azure AD/Entra, Intune/Endpoint Manager, and other cloud services.
- Hands-on experience with troubleshooting and maintaining diverse hardware and software systems (Windows, macOS, iOS, Android, etc.).
- Experience managing VoIP systems and networking equipment in an enterprise setting.
- Strong experience in documentation, reporting, and incident management using tools like Zendesk, ServiceNow, or equivalent platforms.

Desirable Skills:

- Strong problem-solving skills, with the ability to troubleshoot complex technical issues efficiently.
- Excellent verbal and written communication skills, with the ability to explain technical concepts to non-technical users.
- Ability to work well in a team, mentor junior staff, and provide exceptional customer service.
- Highly organized with a focus on detail, ensuring system configurations are accurate and well-documented.
- Proactive in identifying areas for improvement in processes and systems to enhance operational efficiency.
- Ability to work under pressure and manage multiple tasks and priorities simultaneously.

CLIN 03-04 - System Administrator
CLIN 03-12 - System Administrator

Provide maintenance, managing, and optimizing the Court's IT infrastructure, including cloud services, security solutions, collaboration tools, and hardware devices. This role is vital in ensuring that the Court's digital ecosystem is secure, efficient, and aligned with industry best practices. The technician will provide both technical and customer service support, ensuring that issues are promptly resolved, and systems operate smoothly. Requires hands-on expertise in managing hardware, software, and network configurations, as well as providing support to end-users.

Customer Service & User Support

- Offer exceptional customer service and technical support to end users, ensuring their satisfaction and efficient resolution of issues.
- Provide timely and effective troubleshooting for various hardware/software issues, identifying root causes and implementing solutions.
- Utilize a ticketing system (e.g., Zendesk) to track and resolve user-reported incidents and service requests.
- Document resolutions and provide knowledge base updates to improve future support interactions.

- Manage escalations and collaborate with senior technical staff for complex issues.

System Administration & Maintenance:

- Administer and maintain user accounts, permissions, and access control on M365/O365, Azure AD/Entra, and other cloud services.
- Configure and manage Intune/Endpoint Manager for mobile device management and system updates across a variety of devices (Windows, Mac, iOS, Android).
- Oversee user access and permissions on SharePoint and assist in the creation, management, and sharing of documents and resources.
- Monitor and maintain the health of VoIP systems (Poly Phones) and ensure reliable communication for the Court.
- Manage and support systems like Zendesk for ticketing, issue resolution, and communication with internal teams or clients.
- Ensure the proper functioning of security cameras and video management systems like Axis and Eagle **Eye**.
- Administer and maintain systems for Documo mFax, ensuring secure and compliant electronic faxing capabilities.
- Provide support for software and applications in Microsoft Office suite, including troubleshooting and updates.

Device Management and Support

- Manage, troubleshoot, and provide end-user support for both Mac and Windows laptops and iOS/Android smartphones.
- Assist with the setup, configuration, and troubleshooting of hardware and software across various devices.
- Provide end-user training and guidance for effective device and software use, ensuring consistent functionality and security.

Security and Compliance

- Ensure compliance with organizational security policies and procedures for all systems and devices.
- Assist in the implementation of security best practices and monitor for vulnerabilities across the IT infrastructure.
- Perform periodic audits of user access, system configurations, and security logs.

Skills and Qualifications:

Technical Skills

- Proficiency in managing and supporting Microsoft 365/O365, Azure AD, Intune/Endpoint Manager, and SharePoint.
- Experience with managing mobile devices using iOS/Android and handling software updates and troubleshooting on Mac and Windows laptops.
- Expertise in VoIP technology and troubleshooting Poly Phones or similar systems.
- Familiarity with security camera systems like Axis and Eagle Eye and the ability to manage and troubleshoot video surveillance systems.
- Proficient in using and supporting Zendesk for customer service and ticketing processes.
- Familiarity with Documo mFax for secure faxing.
- Basic networking knowledge for troubleshooting internet and cloud connectivity issues.

- Experience with Zoom for virtual communications, troubleshooting meeting issues, and managing settings.

Troubleshooting & Root Cause Analysis

- Diagnose and resolve issues related to software, hardware, network, and system malfunctions.
- Perform root cause analysis to identify the underlying cause of recurring problems, working to eliminate those issues through process or configuration improvements.
- Analyze logs, performance metrics, and error reports to identify and resolve issues proactively.
- Strong troubleshooting skills to quickly and effectively resolve issues across a variety of IT systems and technologies.

Customer Service & Communication Skills:

- Excellent communication and interpersonal skills, with the ability to clearly explain technical information to non-technical users.
- Proven ability to provide high-quality, customer-focused service while resolving issues in a timely and professional manner.
- Strong problem-solving abilities with a focus on root cause analysis.

Certifications

Technical Certifications:

- Microsoft Certified: Azure Fundamentals
- CompTIA A+ Certification (or equivalent)
- CompTIA Network+ Certification (for network troubleshooting)
- Microsoft Certified: Security, Compliance, and Identity Fundamentals
- Apple Certified Support Professional (ACSP) (for Mac laptop support)
- ITIL Foundation Certification (for IT service management)
- Zendesk Certified Administrator (for managing Zendesk systems)
- CompTIA Security+ (for security awareness)

Required Experience:

- Minimum of 5 years of hands-on experience in system administration and technical support.
- Demonstrated experience in M365/O365, Azure AD, Intune, and supporting both Mac and Windows-based systems.
- Experience in troubleshooting a wide range of IT hardware and software, including mobile devices (iOS/Android).
- Proven customer service experience in an IT support capacity, with a track record of successful issue resolution and user satisfaction.
- Familiarity with VoIP systems, Zoom, and security camera systems preferred.

Desirable Skills:

- Strong organizational skills and the ability to prioritize multiple tasks and projects.
- Ability to work independently as well as part of a team in a fast-paced environment.
- Willingness to stay updated on new technologies, certifications, and industry best practices.

CLIN 03-06 - Help Desk Technician

Provide technical support and troubleshooting services to ensure the smooth operation of IT systems and user devices. The role involves diagnosing and resolving technical issues related to a variety of hardware, software, network, and cloud-based systems within a fast-paced IT environment. The technician will be part of a team dedicated to delivering exceptional customer service, ensuring seamless system performance, and supporting a wide range of devices and applications, including Microsoft 365 (M365/O365), Azure AD/Entra, Zendesk, Intune/Endpoint Manager, SharePoint, VoIP systems, and more.

Technical Support & Troubleshooting:

- Provide first-line support to end users via phone, email, and ticketing systems (Zendesk) for technical issues related to hardware, software, and applications.
- Diagnose and resolve technical problems across various platforms, including Windows, macOS, iOS, and Android devices.
- Support M365/O365 apps (Word, Excel, PowerPoint, Teams, etc.), SharePoint, and Intune/Endpoint Manager for device management.
- Troubleshoot network connectivity, VPN issues, and cloud services issues, including Azure AD/Entra and Zoom.
- Manage and support VoIP systems like Poly Phones and address issues related to cloud-based telephony systems.

Customer Service & User Support:

- Deliver exceptional customer service by responding to inquiries and resolving technical issues with professionalism and patience.
- Communicate technical information in a user-friendly manner to non-technical users.
- Maintain a customer-focused attitude, ensuring all issues are handled promptly and with courtesy.

System Administration & Maintenance:

- Assist in the installation, configuration, and maintenance of hardware, software, and devices, including laptops, smartphones, security cameras (Axis, Eagle Eye), and fax systems (Documo mFax).
- Conduct system updates, patches, and upgrades across various platforms, ensuring optimal system performance.
- Monitor and ensure devices are following security policies, including antivirus and endpoint security solutions.

Documentation & Reporting:

- Share technical knowledge and troubleshooting techniques with team members to foster continuous learning and improvement.
- Assist in creating knowledge base articles and self-help resources for end-users.
- Provide training or onboarding support for new employees regarding IT systems and software applications.
- Maintain accurate records of support tickets, issues, resolutions, and inventory.
- Prepare detailed reports on common technical issues and trends to inform proactive system improvements.

- Document standard operating procedures and troubleshooting workflows for internal reference.

Skills & Qualifications:

Technical Skills

- Proficiency in supporting Microsoft 365/O365 suite (Teams, Outlook, OneDrive, SharePoint, etc.).
- Strong working knowledge of Azure Active Directory (AD) / Entra for user and device management.
- Experience with Intune and Endpoint Manager for mobile device and endpoint management.
- Familiarity with cloud-based solutions, including Zoom, VoIP services (e.g., Poly Phones), and related collaboration tools.
- Expertise in troubleshooting Windows and macOS operating systems, including hardware and software issues.
- Solid understanding of mobile device management for iOS and Android smartphones.
- Knowledge of security protocols for protecting user data and systems, including multi-factor authentication (MFA).
- Experience with network troubleshooting (Wi-Fi, VPN, firewalls) and cloud connectivity.
- Hands-on experience with security camera systems (Axis, Eagle Eye).
- Familiarity with virtual private network (VPN) solutions and remote access tools.

Certifications

Technical Certifications:

- Microsoft Certified: Modern Desktop Administrator Associate (or equivalent).
- CompTIA A+ Certification (or equivalent).
- ITIL Foundation Certification.
- Microsoft Certified: Security, Compliance, and Identity Fundamentals.
- Microsoft Certified: Azure Fundamentals.
- Microsoft Certified: Security Operations Analyst Associate.
- Cisco Certified Network Associate (CCNA) or equivalent.
- Any relevant certifications related to Apple macOS, mobile device management, or VoIP services are a plus.

Required Experience:

- Minimum of 5 years of experience in IT support or help desk roles.
- Proven experience troubleshooting and supporting a broad range of IT systems and devices, including laptops, mobile phones, VoIP, and security systems.
- Experience with cloud-based services and systems, such as M365/O365, Azure AD, Intune, and SharePoint.
- Prior experience with ticketing systems like Zendesk or similar platforms.
- Hands-on experience with a mix of both Windows and macOS operating systems.

Desirable Skills:

- Strong analytical and problem-solving skills, with an ability to prioritize tasks in a fast-paced environment.
- Excellent written and verbal communication skills, with the ability to explain complex technical issues in simple terms.
- Strong attention to detail and organizational skills.
- Ability to work both independently and as part of a collaborative team.
- A proactive and self-motivated approach to continuous learning and staying updated on emerging technologies.

CLIN 03-07 – Jr. Help Desk Technician:

The Junior Help Desk Technician provides first-line technical support for end users, assisting with basic troubleshooting, system issues, and IT support requests. This role is ideal for individuals looking to gain hands-on experience in IT support while developing expertise in hardware, software, and network troubleshooting. The technician will work under the guidance of senior team members to resolve issues and ensure smooth operation of IT systems and devices.

Technical Support & Troubleshooting:

- Provide entry-level IT support for hardware, software, and application issues via phone, email, and ticketing systems (e.g., Zendesk).
- Assist users with basic troubleshooting for Windows and macOS operating systems.
- Support common office applications, including Microsoft 365 (Word, Excel, Teams, Outlook, SharePoint, OneDrive, etc.).
- Help resolve network connectivity issues, such as Wi-Fi and VPN access problems.
- Provide initial troubleshooting for VoIP phones, cloud-based applications, and security systems under supervision.
- Escalate complex technical issues to senior technicians or specialized teams as needed.

Customer Service & User Support:

- Deliver friendly and professional IT support, ensuring a positive user experience.
- Explain technical concepts in clear, simple terms to non-technical users.
- Document solutions and contribute to internal knowledge base articles for future reference.

System Administration & Maintenance:

- Assist in setting up laptops, desktops, and mobile devices (Windows, macOS, iOS, Android).
- Follow standard procedures to install and update software, security patches, and system configurations.
- Ensure compliance with basic IT security policies, including password resets and multi-factor authentication (MFA) setup.
- Support asset management by maintaining accurate records of IT equipment and devices.

Skills & Qualifications:

Technical Skills

- Basic knowledge of Microsoft 365 applications (Teams, Outlook, Word, Excel, etc.).
- Familiarity with Windows and macOS troubleshooting.

- Basic understanding of network connectivity issues, including Wi-Fi and VPN.
- Strong problem-solving skills with a willingness to learn.
- Excellent communication and customer service skills.
- Ability to follow instructions and escalate issues appropriately.

Certifications:

Technical Certifications

- CompTIA A+ Certification (or equivalent entry-level IT certification).
- Microsoft 365 Fundamentals (MS-900)

Required Experience:

- Minimum of two years of experience in IT support, help desk, or related technical role are required.
- Internship, coursework, or part-time IT roles are acceptable for experience.
- Some hands-on experience with troubleshooting hardware and software issues is preferred but not required.

Desirable Skills:

- Exposure to help desk ticketing systems (e.g., Zendesk, ServiceNow).
- Experience with mobile device setup (iOS, Android).
- Interest in learning about cloud services (Azure AD, Intune, SharePoint).

CLIN 03-09 - Help Desk Engineer

Provide essential technical support and troubleshooting services to ensure the smooth operation of the IT environment within the Court. This role serves as the primary point of contact for internal employees experiencing IT-related issues, offering expert assistance across a broad range of technologies. The Help Desk Engineer is responsible for diagnosing and resolving technical problems, maintaining systems, providing exceptional customer service, and contributing to the efficiency of IT operations and a dynamic environment. The ideal candidate is highly proficient in Microsoft 365 (M365), Azure Active Directory (Azure AD), Intune/Endpoint Manager, SharePoint, and other tools while possessing strong communication and problem-solving skills.

Technical Support & Troubleshooting:

- Provide first-line support for a wide variety of technologies, including but not limited to M365/O365, Azure AD/Entra, SharePoint, Intune, VoIP systems, and endpoint devices.
- Troubleshoot issues related to hardware, software, and network connectivity on Windows laptops, Mac laptops, iOS/Android smartphones, and other devices.
- Diagnose, identify, and resolve technical problems in a timely manner, escalating complex issues to senior engineers or other specialized teams as needed.
- Manage user accounts, permissions, and security settings in M365, Azure AD/Entra, and other internal platforms.

Customer Service & User Report:

- Deliver exceptional customer service by ensuring that end-users receive clear, friendly, and professional assistance.

- Prioritize and manage help desk tickets efficiently, ensuring that each issue is resolved within the Service Level Agreement (SLA).
- Communicate technical information effectively to non-technical users.
- Maintain a calm, helpful demeanor during troubleshooting and issue resolution, especially when working under pressure.

System Administration & Maintenance:

- Regularly monitor and maintain the health of the IT environment, including ensuring that systems are up-to-date, secure, and compliant.
- Perform updates and patches on hardware, software, and cloud services (e.g., M365, SharePoint, Azure AD).
- Assist in the deployment of new hardware, software, and IT infrastructure.

Documentation & Reporting:

- Document troubleshooting steps, solutions, and best practices for internal knowledge sharing.
- Create and update technical documentation for both end users and IT staff.
- Produce regular reports regarding system performance, common issues, and support metrics.

Skills & Qualifications:

- Strong understanding of Microsoft 365/O365 services, including Exchange, Teams, SharePoint, OneDrive, and Outlook.
- Expertise in managing users, groups, and roles within Azure Active Directory (Azure AD) and Entra.
- Knowledge of Intune/Endpoint Manager for device management and security enforcement.
- Familiarity with various endpoint devices such as Windows laptops, Mac laptops, iOS and Android smartphones.
- Experience with VoIP systems such as Poly Phones and other communication platforms like Zoom.
- Basic understanding of security camera systems, such as Axis and Eagle Eye, and their integration with IT environments.
- Knowledge of cloud-based services and troubleshooting methods, including VPNs, network connectivity, and cloud storage.

Certifications:

- Microsoft Certified: Security, Compliance, and Identity Fundamentals (or higher) or similar certifications.
- Microsoft Certified: Azure Fundamentals (or higher).
- CompTIA A+ or similar entry-level IT certification.
- ITIL Foundation certification (desirable for understanding IT service management principles).
- Microsoft Certified: Azure Administrator Associate or Microsoft Certified: Modern Desktop Administrator Associate.
- CompTIA Network+ or similar networking certification.

- Certified Information Systems Security Professional (CISSP) or similar security certification.
- Zendesk Support Administrator certification (preferred, for Zendesk-specific environments).

Required Experience:

- Minimum of 3 years of experience in a help desk or IT support role with a focus on troubleshooting and user support.
- Hands-on experience with M365/O365, SharePoint, and Azure AD/Entra administration.
- Experience with mobile device management (MDM), preferably Intune.
- Familiarity with cloud-based systems, such as Zoom, VoIP systems (e.g., Poly Phones), and other communication platforms.
- Experience with ticketing systems, preferably Zendesk, for tracking and resolving service requests.

Desirable Skills:

- Strong interpersonal and communication skills, with the ability to collaborate with both technical and non-technical team members.
- Excellent time management skills and the ability to prioritize competing tasks effectively.
- Strong problem-solving ability, with a focus on troubleshooting and finding quick resolutions.
- Ability to work under pressure and manage multiple priorities.
- High level of attention to detail, ensuring all systems are functioning optimally and securely.
- A customer-focused mindset, ensuring that all end-users are supported in a friendly and timely manner.

CLIN 03-10 Jr. Help Desk Engineer

The Junior Help Desk Engineer is responsible for providing first-level technical support, troubleshooting, and IT assistance to end users. This role requires foundational knowledge of enterprise IT systems, including user account management, endpoint troubleshooting, and network connectivity. The engineer will assist in maintaining IT infrastructure, ensuring system security, and supporting enterprise applications within a structured IT environment.

Technical Support & Troubleshooting:

- Provide first-line technical support for IT-related issues, including hardware, software, and network connectivity.
- Diagnose and resolve issues on Windows and macOS endpoints, as well as iOS and Android mobile devices.
- Support enterprise applications, including Microsoft 365 (Exchange, Teams, SharePoint, OneDrive).
- Manage user accounts, permissions, and authentication settings within Azure Active Directory (Azure AD/Entra).
- Troubleshoot network connectivity issues, including VPN, Wi-Fi, and cloud-based services.

- Support VoIP systems, including Poly Phones and cloud-based telephony solutions.
- Identify and escalate complex issues to higher-tier engineers with appropriate documentation.

System Administration & Maintenance:

- Assist in the deployment and configuration of new user workstations, software installations, and system updates.
- Ensure compliance with IT security policies, including antivirus, endpoint protection, and multi-factor authentication (MFA).
- Support mobile device management (MDM) through Microsoft Intune/Endpoint Manager.
- Monitor and maintain IT infrastructure, ensuring availability and performance of essential systems.
- Conduct routine system checks and maintenance tasks to enhance system stability.

Documentation & Reporting

- Maintain accurate records of incidents, troubleshooting steps, and resolutions within the IT ticketing system.
- Assist in developing and updating technical documentation, standard operating procedures (SOPs), and knowledge base articles.
- Provide reporting on recurring issues, system performance, and support trends to optimize IT operations.

Skills & Qualifications:

- Strong foundational knowledge of Microsoft 365 services (Exchange, Teams, SharePoint, OneDrive).
- Basic proficiency in Active Directory and Azure AD/Entra user management.
- Understanding of networking concepts, including TCP/IP, VPNs, and Wi-Fi troubleshooting.
- Experience with Windows and macOS endpoint troubleshooting.
- Familiarity with cloud-based IT environments and enterprise collaboration tools.
- Ability to diagnose and resolve common IT issues with a structured approach.
- Strong analytical and problem-solving skills with attention to detail.

Certifications:

- CompTIA A+ or IT Fundamentals+
- Microsoft Certified: Security, Compliance, and Identity Fundamentals
- Microsoft Certified: Azure Fundamentals

Required Experience:

- Minimum of 2 years of experience in IT support, help desk, or related technical role are required.
- Internship, coursework, or part-time IT roles are acceptable for experience.

Desirable Skills:

- Experience with IT ticketing systems such as Zendesk or ServiceNow.

- Exposure to Intune/Endpoint Manager for device provisioning and compliance management.
- Familiarity with VoIP systems and cloud-based communication platforms such as Zoom.
- Knowledge of IT security best practices, including MFA, endpoint security, and data protection

CLIN 03-13 Jr. System Administrator

The Junior/Entry-Level IT Support Technician assists in maintaining and troubleshooting the Court's IT infrastructure, including hardware, software, cloud services, and security systems. This role provides hands-on technical support to end-users, ensuring smooth operations across various IT systems. The technician will work under supervision to resolve technical issues, manage user accounts, and maintain system security while gaining valuable experience in IT support and administration.

Customer Service & User Support:

- Respond to user requests for technical assistance, ensuring a positive customer experience.
- Log and track IT support requests using a ticketing system (e.g., Zendesk).
- Document resolutions and contribute to a knowledge base for future support.
- Escalate complex issues to senior IT staff when necessary.

System Administration & Maintenance:

- Assist in managing user accounts, permissions, and access controls in Microsoft 365 (M365/O365) and Azure Active Directory (Entra).
- Support the configuration and management of mobile devices using Intune/Endpoint Manager.
- Help with user access and permissions on SharePoint, including document sharing and organization.
- Monitor VoIP systems and provide basic troubleshooting for communication issues.
- Assist with ticket management and issue tracking in Zendesk or similar help desk platforms.
- Provide basic support for security cameras and video management systems like Axis and Eagle Eye.
- Help manage electronic faxing systems such as Documo mFax.
- Support Microsoft Office applications and assist users with troubleshooting common software issues.

Device Management & Support:

- Assist with setting up, configuring, and troubleshooting Windows and Mac laptops, as well as iOS and Android smartphones.
- Provide basic troubleshooting for hardware and software issues across different devices.
- Support end-users by answering IT-related questions and helping them use various tools and systems effectively.

Security & Compliance:

- Follow security best practices, including managing multi-factor authentication (MFA) and data protection policies.

- Assist with user access audits and security compliance checks.
- Help monitor for potential security vulnerabilities and report concerns to senior staff.

Skills & Qualifications

Technical Skills:

- Basic knowledge of Microsoft 365/O365, Azure AD, and Intune/Endpoint Manager.
- Familiarity with Windows and Mac operating systems and mobile device management.
- Basic understanding of VoIP systems and IT ticketing tools (e.g., Zendesk).
- Ability to troubleshoot common hardware and software issues.
- Basic networking knowledge for troubleshooting connectivity problems.
- Familiarity with collaboration tools like Zoom and Microsoft Teams.

Troubleshooting & Root Cause Analysis:

- Assist in diagnosing basic software, hardware, and network issues.
- Support troubleshooting efforts by analyzing logs and error reports under supervision.
- Contribute to problem resolution by applying standard troubleshooting techniques.
- Ability to diagnose basic IT issues and escalate more complex problems.
- Willingness to learn root cause analysis techniques for improving system reliability.

Customer Service & Communication Skills:

- Strong communication skills with the ability to explain technical issues to non-technical users.
- A customer-oriented mindset with a focus on providing efficient IT support.
- Willingness to learn and adapt in a fast-paced IT environment.
- Strong organizational skills and ability to prioritize tasks.
- Willingness to learn new technologies and pursue relevant IT certifications.
- Ability to work both independently and as part of a team.

Certifications:

- CompTIA A+ Certification (Entry-level IT support and troubleshooting)
- CompTIA Network+ Certification (Basic networking knowledge)
- Microsoft Certified: Azure Fundamentals
- ITIL Foundation Certification (IT service management best practices)

Required Experience:

- Minimum of 2 years of experience in IT support, help desk, or a related technical role.
- Hands-on experience with troubleshooting hardware, software, and network issues (academic, internship, or work experience).
- Familiarity with Microsoft 365, Windows/Mac operating systems, and basic IT infrastructure concepts.
- Previous experience in a customer service or technical support role is a plus.

H.4.3 Strategic IT Initiatives Segment LCAT Descriptions

CLIN 04-01 Cloud Network Solutions Architect
CLIN 04-13 Cloud Network Solutions Architect

Entrusted of designing, implementing, and optimizing cloud-based solutions to meet the business objectives of our Court and clients. Your contributions will be vital in supporting scalable, secure, and high-performance network architectures that align with modern cloud technologies.

Key Responsibilities:

- **Cloud Network Design, Architecture, and Implementation:** Design and implement hybrid network solutions using cloud platforms, and premises infrastructure ensuring they meet performance, scalability, and security requirements.
- **On-premises Infrastructure Design, Architecture, and Implementation:** Design, implement, and maintain the on-prem network solution including network and low power cabling repair, troubleshooting and resolving on-prem issues (e.g., Point of Sale System, Video Surveillance System, Physical Access Control System, Voice Over IP (VoIP) System, network (LAN and WAN) equipment, hypervisor, servers)
- **Solution Delivery:** Collaborate with internal teams and stakeholders to understand the business needs and gather technical requirements, architect network solutions, and deliver end-to-end implementation plans.
- **Cloud Security:** Ensure cloud network infrastructure adheres to security best practices, including encryption, access controls, contribute to risk assessments and ensure relevant regulatory compliance.
- **Troubleshooting & Optimization:** Analyze and troubleshoot network issues (on-prem, in the cloud), optimize performance, and ensure high availability for cloud networks.
- **Collaboration & Support:** Work closely with DevOps, NetOps, SecOps, SysOps Teams to integrate network solutions with cloud applications and services.
- **Documentation & Best Practices:** Maintain thorough documentation of network architectures, designs, and best practices to support internal knowledge sharing, processes for operational use.
- **Continuous Learning:** Stay up to date with emerging cloud networking technologies, trends, and tools to continually research, recommend & improve solutions and processes.

Skills & Qualifications:

- Solid understanding of cloud networking principles, including VPCs, load balancers, DNS, and routing.
- Hands-on experience with at least one major cloud platform such as AWS (e.g., EC2, S3, VPC, Lambda) or Azure (e.g., Virtual Networks, Azure Firewall, Azure Functions).

- Familiarity with network protocols (TCP/IP, BGP, OSPF, etc.) and network security technologies.
- Exposure to infrastructure-as-code tools such as Terraform, CloudFormation, or Ansible.
- Practical experience with technologies like Cisco UCS-C servers, Microsoft Hyper-V, RedHat Linux, and uninterruptible power supplies.
- Knowledge of environmental monitors, physical access control systems, video camera surveillance systems, intercoms, and portable network kits.
- Experience with VoIP systems (e.g., Poly phone), printers, scanners, kiosks, and point-of-sale systems.
- Familiarity with Windows Server and solutions such as GitHub, Zscaler, CrowdStrike, and Security Information & Event Management (SIEM) platforms (e.g., Splunk).
- Strong problem-solving and troubleshooting skills.
- Effective communication and teamwork abilities.
- Climbing ladders, lifting heavy equipment (e.g., racking equipment), crawling under desks, etc.
- Ability to manage tasks and priorities in a dynamic environment.

Certifications:

- AWS Certified Solutions Architect – Associate or Professional
- Microsoft Azure certified – Associate or Expert
- CompTIA certified: Network+ or Security+ or Server+ or Cloud+

Required Experience:

- Minimum of 7 years of experience in network engineering or related roles.
- Minimum of 5 years of experience with cloud network solutions in professional services.
- Experience contributing to cloud networking projects
- Experience contributing to cloud application projects.
- Experience contributing to cloud automation projects
- Experience contributing to hybrid networking projects.
- Familiarity with Agile environment

Education:

- Bachelor's degree in computer science, Information Technology, or a related field is preferred.
- Relevant work experience may substitute for formal education.

CLIN 04-02 Cloud Network Systems Engineer
CLIN 04-16 Cloud Network Systems Engineer

Responsible for designing, implementing, and managing cloud infrastructure and networking solutions to ensure high performance, scalability, and security for the Cloud's cloud environment. This role combines expertise in cloud technologies with a deep understanding of network systems, helping to optimize cloud resources, manage network configurations, and ensure a seamless connection between on-premises and cloud-based systems.

Key Responsibilities:

- **Cloud Infrastructure Design & Implementation**: Design, deploy, and maintain cloud-based network solutions that integrate with existing on-premises infrastructure.
- **On-prem Infrastructure Design, Architecture, and Implementation:** Design, implement, and maintain the on-prem network solution including network and low power cabling repair, troubleshooting and resolving on-prem issues (e.g., Point of Sale System, Video Surveillance System, Physical Access Control System, Voice Over IP (VoIP) System, network (LAN and WAN) equipment, hypervisor, servers)
- **Network Configuration & Management**: Configure, monitor, and troubleshoot network systems within cloud environments, ensuring optimal performance and reliability.
- **Collaboration & Consultation**: Work closely with cloud architects, security teams, and other stakeholders to ensure cloud infrastructure meets business needs.
- **Automation & Optimization**: Implement automation and orchestration tools to streamline network management processes and optimize resource usage.
- **Security & Compliance**: Ensure security policies and standards are met within cloud networks, including implementing firewalls, VPNs, and encryption measures.
- **Troubleshooting & Support**: Provide ongoing support for network-related issues in cloud environments, resolving technical challenges and ensuring minimal downtime.
- **Monitoring & Reporting**: Use monitoring tools to track network performance and provide regular reports to management and teams on the health of cloud network infrastructure.

Skills & Qualifications:

- Practical experience with cloud platforms such as AWS, Microsoft Azure, Datacenter
- Knowledge of cloud security practices, including securing data transmission and access control
- Experience with networking protocols and network security technologies (e.g., TCP/IP, DNS, routing, firewalls, VPNs, etc.).
- Familiarity with network automation tools and scripting languages like Python, Ansible, or Terraform or similar
- Familiarity with cloud-specific networking services (e.g., VPC, Direct Connect, Cloud VPN, Load Balancers, etc.).
- Experience with network monitoring tools
- Familiarity with Windows Server and software tools like GitHub, Zscaler, CrowdStrike, and SIEM platforms (e.g., Splunk).

- Practical experience with technologies like Cisco UCS-C servers, Microsoft Hyper-V, RedHat Linux, and uninterruptible power supplies.
- Knowledge of environmental monitors, physical access control systems, video camera surveillance systems, intercoms, and portable network kits.
- Experience with VoIP systems (e.g., Poly phone), printers, scanners, kiosks, and point-of-sale systems.
- Strong analytical, problem-solving and communication skills.
- Proficient in troubleshooting network issues, diagnosing root causes, and resolving problems effectively.
- Demonstrate individual initiatives, contribution and collaboration abilities.
- Climbing ladders, lifting heavy equipment (e.g., racking equipment), crawling under desks, etc.
- Ability to manage tasks and priorities in a dynamic environment.

Certifications:

- AWS Certified – Foundational, Associate or Specialty
- Microsoft Azure Certified – Associate or Expert
- CompTIA certified: Network+ or Security+ or Server+ or Cloud+

Required Experience:

- Minimum of 7 years in network engineering, cloud infrastructure, or a related role.
- Proven track record of designing and managing cloud-based or hybrid networking solutions.
- Experience working with hybrid cloud environments and multi-cloud setups is a plus.
- Previous experience with large-scale infrastructure projects or working in a DevOps or cloud engineering team.

Education:

- Bachelor's degree in computer science, Information Technology, or a related field is preferred
- Relevant work experience may substitute for formal education.

CLIN 04–03 Cloud Network Operations Administrator
CLIN 04–19 Cloud Network Operations Administrator

Key role in the management, monitoring, and optimization of cloud-based network infrastructure. This individual will work closely with cross-functional teams to ensure seamless operations of cloud network environments and services. The ideal candidate will have experience working with cloud platforms such as AWS, Azure, on-premises infrastructure, and will possess strong troubleshooting and problem-solving skills to maintain high availability, security, and performance of hybrid network infrastructures.

Key Responsibilities:

- **Incident Management:** Troubleshoot and resolve cloud network-related incidents and issues, ensuring minimal downtime and prompt service restoration.

- **Administration of On-prem Infrastructure:** daily administration of on-prem systems and network appliances including cabling, servers, hypervisor, Point of Sale System, Video Surveillance System, Physical Access Control System, Voice Over IP (VoIP) System, network (LAN and WAN) equipment.
- **Performance Monitoring:** Implement and monitor performance metrics for cloud networks, ensuring optimal performance, scalability, and efficiency.
- **Automation & Scripting:** Develop and maintain automation scripts to streamline cloud network provisioning, configuration, and monitoring processes.
- **Security and Compliance:** Work with security teams to ensure the cloud network architecture adheres to security best practices and compliance standards.
- **Documentation:** Maintain detailed documentation for network configurations, processes, and procedures related to cloud network operations.
- **Collaboration:** Work collaboratively with other IT teams, cloud architects, and developers to integrate cloud network solutions into broader infrastructure strategies.
- **Support Cloud Network Deployments:** Assist in the planning and deployment of cloud-based network solutions and services for new and ongoing projects.
- **Troubleshooting and Support:** Provide mid-level support for day-to-day operational issues within the cloud network infrastructure, ensuring continuity of service for business-critical applications.

Skills & Qualifications:

- Proficient in network operations and system operations, ideally in a hybrid network environment.
- Hands-on experience with cloud platforms (AWS, Azure and related services.
- Hands-on experience with hybrid network infrastructure and related services.
- Hands-on experience with on-premises network infrastructure and related services.
- Proficiency in network protocols (TCP/IP, DNS, HTTP/HTTPS, ...) and security technologies (Firewall, VPNs).
- Experience with monitoring tools and cloud infrastructure management (e.g., CloudWatch, Azure Monitor, Prometheus).
- Familiarity with automation and scripting tools (e.g., Python, PowerShell, Terraform).
- Knowledge of security best practices and tools.
- Excellent troubleshooting skills
- Climbing ladders, lifting heavy equipment (e.g., racking equipment), crawling under desks, etc.
- Strong communication skills and ability to collaborate with multiple teams.
- Understanding of networking concepts such as VPN, SD-WAN and DNS.

Certifications:

- AWS or Azure Cloud certifications such as AWS Certified Solutions Architect, Azure Network Engineer
- CompTIA Certified – Network+ Server + Cloud+
- ITIL Foundation Certification

Required Experience:

- Minimum of 5 years of experience in network engineering or network operations, with a focus on cloud environments.
- Familiarity with containerization and microservices networking (Kubernetes, Docker).
- Experience with hybrid cloud environments or multi-cloud setups.
- Hands-on experience with cloud platforms (AWS, Azure) and related networking services.
- Hands-on experience with hybrid network infrastructure and related networking services.
- Hands-on experience with on-premises network infrastructure and related networking services.
- Proven experience with cloud-based network troubleshooting and performance optimization.
- Experience in managing hybrid or multi-cloud network environments is a plus.
- Previous experience with network automation and scripting tools preferred.

Education:

- Bachelor's degree in computer science, Information Technology, or a related field is preferred.
- Relevant work experience may substitute for formal education.

CLIN 04-04 - UX Researcher / Designer
CLIN 04-21 - UX Researcher / Designer

User Experience and mobile/desktop design experience with an emphasis on accessibility/usability testing.

- **Communication and Collaboration**: have effective communication skills and the ability to collaborate within a team environment, including sharing progress, asking for help when needed, and providing constructive feedback.
- **Continuous Learning**: have an eagerness to learn and adapt to new technologies, frameworks, and best practices in web development.
- **Skills & Qualifications**:
    - User Research: ability to conduct and analyze user research, interviews, and surveys.
    - Wireframing and Prototyping: creating basic blueprints of design layouts and interactive prototypes in tools like Figma, Sketch, Adobe XD, etc.
    - Visual Design: Knowledge of font choices, color schemes, and how they impact user experience as well as an understanding of grid systems, balance, and visual hierarchy.
    - Interactive Design: designing smooth transitions, animations, and feedback loops as well as designs that work well across different devices and screen sizes.
    - Information Architecture: structuring information in a way that is logical and easy to navigate and creating intuitive navigation systems.

- Design Tools: Proficiency in tools like Figma, Sketch, Adobe Creative Suite as well as basic HTML/CSS knowledge.
- Usability Testing: Planning and conducting tests to validate design decisions and the ability to refine designs based on feedback and test results.
- Problem-Solving and Critical Thinking: Approaching design challenges with the user's needs in mind and taking an iterative approach towards refining designs and ideas.
- Attention to Detail: Ensuring every element is perfectly aligned and visually consistent, and the design language is consistent throughout the product or suite of products.

- **Education:**
  - Bachelor's or equivalent work experience
- **Required Experience:**
  - Minimum of 4 years of experience with user research, wireframing, prototyping, and visual design.
  - Minimum of 4 years of experience using design tools such as Figma, Sketch, or Adobe XD.
  - Minimum of 4 years of experience using design systems, usability principles, and accessibility standards (WCAG).
  - Minimum of 4 years of experience on software projects that involved conducting user interviews, surveys, A/B testing, and heuristic evaluations to drive design decisions.

CLIN 04-05 – Web Designer
CLIN 04-22 – Web Designer

Graphic designer with a solid understanding of visual design principles, user experience (UX), and modern web technologies, responsible for designing aesthetically appealing and functional websites, web components, and user interfaces.

- **Communication and Collaboration**: have effective communication skills and the ability to collaborate within a team environment, including sharing progress, asking for help when needed, and providing constructive feedback.
- **Continuous Learning**: have an eagerness to learn and adapt to new technologies, frameworks, and best practices in web development.
- **Technology Knowledge**: maintain knowledge and skills on existing and emerging agile best practices, technologies relevant to supported projects, security best practices, etc.
- **Skills & Qualifications:**
  - Wireframing and Prototyping: creating basic blueprints of design layouts and interactive prototypes in tools like Figma, Sketch, Adobe XD, etc.
  - Visual Design: Knowledge of font choices, color schemes, and how they impact user experience as well as an understanding of grid systems, balance, and visual hierarchy.

- Interactive Design: designing smooth transitions, animations, and feedback loops as well as designs that work well across different devices and screen sizes.
- Information Architecture: structuring information in a way that is logical and easy to navigate and creating intuitive navigation systems.
- Design Tools: Proficiency in tools like Figma, Sketch, Adobe Creative Suite as well as basic HTML/CSS knowledge.
- Problem-Solving and Critical Thinking: Approaching design challenges with the user's needs in mind and taking an iterative approach towards refining designs and ideas.
- Attention to Detail: Ensuring every element is perfectly aligned and visually consistent, and the design language is consistent throughout the product or suite of products.

- **Education:**
  - Bachelor's or equivalent work experience
- **Required Experience:**
  - Minimum of 4 years of experience with visual design, UI/UX principles, and responsive web design.
  - Minimum of 4 years of experience using tools like Figma, Adobe XD, or Sketch.
  - Minimum of 4 years of experience with design systems, typography, color theory, and accessibility standards (WCAG).
  - Minimum of 2 years of experience with basic HTML and CSS.

CLIN 04-06 – Office 365 Engineer
CLIN 04-23 – Office 365 Engineer

The Office 365 Engineer is a builder and contributor that creates automations to eliminate tedious manual processes, connecting applications with Microsoft Azure resources, and harnessing power of the Microsoft Office suite to better serve Court staff.

- **Continuous Learning**: have an eagerness to learn and adapt to new technologies, frameworks, and best practices within Microsoft 365.
- **Technology Knowledge**: maintain knowledge and skills on existing and emerging agile best practices, technologies relevant to supported projects, security best practices, etc.
- **Skills & Qualifications:**
  - **PowerShell:** Experience and proficiency for integrating with Azure AD, bulk updates across Office 365 services, managing Exchange Online, SharePoint Online, and Microsoft Teams configurations, and automating administrative tasks.
  - **JavaScript/TypeScript:** Experience and proficiency in JavaScript and/or TypeScript.
  - **Python:** Experience and familiarity with using Python for building automation

scripts or performing data analysis.

- **Version Control:** Experience with version control systems like Git for collaborative development and managing codebase changes.
- **Microsoft/Azure Services:** Developed understanding with core Microsoft 365 and Azure Services:
  - Azure Active Directory / Azure Entra
  - PowerPlatform solutions
  - Dataverse
  - Enterprise Applications
  - SharePoint
- **API Integration:** Ability to integrate RESTful APIs endpoints for a client to fetch and manipulate data.
- **Debugging and Testing:** Proficiency in debugging applications as well as writing unit and integration tests using libraries like Jest, React Testing Library, and pytest.

- **Education:**
  - Bachelor's or equivalent work experience
- **Required Experience:**
  - Minimum of 2 years of experience with PowerPlatform Solutions including PowerAutomate and PowerApps, managing environments, deployments and troubleshooting
  - Minimum of 2 years of experience managing SharePoint Sites

CLIN 04-07 Software Quality Assurance Engineer
CLIN 04-24 Software Quality Assurance Engineer

Responding to user support requests and feedback, researching user needs, setting and maintaining quality standards by QA testing, and developing product training materials.

- **Communication and Collaboration**: have effective communication skills and the ability to collaborate within a team environment, including sharing progress, asking for help when needed, and providing constructive feedback. Participate in agile ceremonies.
- **Technology Knowledge**: maintain knowledge and skills on existing and emerging agile best practices, technologies relevant to supported projects, security best practices, etc.
- **Test Automation:**
  - Develop and maintain automated test scripts using appropriate tools
  - Execute automated tests and analyze test results.
  - Write test cases and maintain test case library
- **Issue Tracking and Resolution:**

- Investigate and troubleshoot software defects reported by end-users.
- Monitor and track bug fixes and resolution progress.

- **Quality Assurance Processes:**
  - Participate in the improvement of software quality assurance processes and methodologies.
  - Stay abreast of industry best practices and emerging testing technologies.
  - Contribute to the creation and maintenance of testing documentation

- **Skills & Qualifications**:
  - **Software Testing:** Strong knowledge of manual and automated testing methodologies.
  - **Automation Tools:** Experience with testing frameworks like **Selenium, Cypress, or Playwright.**
  - **Programming Knowledge:** Experience with **Python, JavaScript, or C#** for test automation scripting.
  - **Test Management Tools:** Familiarity with tools like **MondayDev**, **GitHub, TestRail, or Zephyr** for test case management.
  - **API Testing:** Experience using **Postman, REST Assured, or SoapUI** for API testing.
  - **Performance Testing:** Understanding of tools like **Artillery, JMeter, Gatling, or LoadRunner** to test application scalability and speed.
  - **CI/CD Pipelines:** Experience integrating tests into **CI/CD workflows** using Jenkins, GitHub Actions, CircleCI, or GitLab CI.
- **Education:**
  - Bachelor's or equivalent work experience
- **Certifications:**
  - At least one foundational level certification from a reputable trainer such as Certified Associate in Software Testing (CAST) or Certified Software Tester (CSTE)
- **Required Experience:**
  - Minimum of 4 years of experience with software testing, including manual and automated testing, testing tools like Selenium, Cypress, or Playwright for automation, along with experience in API testing using tools like Postman or Jmeter, and test case tools like TestRails.

CLIN 04-08 – Delivery Manager
CLIN 04-25 – Delivery Manager

Managing team resources, identifying blockers and tackled, and ensuring delivery of solutions.

- **Communication and Collaboration**: have effective communication skills and the ability to collaborate within a team environment, including sharing progress, asking for help when needed, and providing constructive feedback.

- **Technology Knowledge**: maintain knowledge and skills on existing and emerging agile best practices, technologies relevant to supported projects, security best practices, etc.
- **Skills & Qualifications**:
    - **Project Management:** Agile (Scrum, Kanban, SAFe), Github Issues, Monday.com, Jira
    - **Delivery Planning:** Roadmap creation, sprint planning, backlog prioritization.
    - **Stakeholder Management:** Communication with executives, customers, and tech teams.
    - **Risk & Issue Management:** Identifying bottlenecks and mitigating risks proactively.
    - **Process Optimization:** Continuous improvement using retrospectives, OKRs, and KPIs.
    - **Budgeting & Resource Allocation:** Managing costs and team capacity.
    - **Technical Awareness:** Understanding software development, DevOps, cloud, and CI/CD (not hands-on but enough to communicate effectively with engineers).
- **Education:**
    - Bachelor's or equivalent work experience
- **Required Experience:**
    - Minimum of 4 years of experience managing teams of developers, working with stakeholders, and delivering software projects using Agile methodologies.

CLIN 04-09 – DevOps Engineer
CLIN 04-26 – DevOps Engineer

Backend engineer with specialty of ensuring application deployment, automated continuous integration testing, and ensuring visibility of performance and key metrics to inform developers' decision making.

- **Communication and Collaboration**: have effective communication skills and the ability to collaborate within a team environment, including sharing progress, asking for help when needed, and providing constructive feedback.
- **Continuous Learning**: have an eagerness to learn and adapt to new technologies, frameworks, and best practices in web development and cloud infrastructure management.
- **Technology Knowledge**: maintain knowledge and skills on existing and emerging agile best practices, technologies relevant to supported projects, security best practices, etc.
- **Skills & Qualifications:**
    - Version Control: Experience with version control systems like Git for collaborative development and managing codebase changes.
    - Terraform: Basic understanding of Infrastructure as Code (IaC) principles and experience with Terraform for provisioning and managing infrastructure resources on cloud platforms such as AWS, Azure, or Google Cloud Platform.

- **CI/CD Pipelines:** GitHub Actions, CircleCI, GitLab CI/CD, ArgoCD, Jenkins.
- **Scripting & Automation** – Python, Bash, Go, PowerShell.
- **Linux & System Administration** – File systems, process management, performance tuning.
- AWS Services: Familiarity with core AWS services such as:
  - AWS Lambda for serverless functions
  - AWS S3 for storage
  - AWS API Gateway for creating RESTful APIs
  - AWS DynamoDB for NoSQL database
  - AWS EC2 for virtual servers
  - AWS RDS for managed relational databases
  - AWS CloudFront for content delivery
  - AWS CloudWatch for Application Monitoring
- **Database Management** – PostgreSQL, MySQL, MongoDB, Redis.

- **Education:** Bachelors in computer science or equivalent work experience
- **Certifications:**
  - AWS Certified DevOps Engineer
- **Required Experience:**
  - Minimum of 5 years of experience working with AWS, infrastructure as code (Terraform, CloudFormation, etc.), CI/CD pipelines (GitHub Actions, CircleCI, etc.), containerization (Docker, Kubernetes, etc.), and scripting (Python, Bash, etc.).
  - Minimum of 3 years of experience working with TypeScript/JavaScript.

CLIN 04-10 – Senior Web Developer
CLIN 04-27 – Senior Web Developer

Full-Stack Developer with expertise in TypeScript, Node.js, React.js, Python, Terraform, CSS, and AWS Services.

- **Technology Knowledge**: maintain knowledge and skills on existing and emerging agile best practices, technologies relevant to supported projects, security best practices, etc.
- **Skills & Qualifications:**
  - JavaScript/TypeScript: Experience and proficiency in JavaScript and/or TypeScript.
  - React.js: Working knowledge of React.js library for building user interfaces and Single Page Applications (SPAs).
  - HTML/CSS: Mastery of HTML and CSS for structuring and styling web pages.
  - Node.js: Proficiency with Node.js for building server-side applications and handling dependencies with tools like npm or yarn.
  - Python/pytest: Experience with Python for building packages and solutions as well as writing unit tests and integration tests.
  - Version Control: Experience with version control systems like Git for collaborative development and managing codebase changes.

- Terraform: Basic understanding of Infrastructure as Code (IaC) principles and experience with Terraform for provisioning and managing infrastructure resources on cloud platforms such as AWS, Azure, or Google Cloud Platform.
- AWS Services: Familiarity with core AWS services such as:
  - AWS Lambda for serverless functions
  - AWS S3 for storage
  - AWS EC2 for virtual servers
  - AWS RDS for managed relational databases
  - AWS CloudFront for content delivery
  - AWS CloudWatch for Application Monitoring
- Microsoft Azure / Office 365:
  - SharePoint for file, web part, and list management
- API Integration: Ability to integrate RESTful APIs endpoints with the React frontend to fetch and manipulate data.
- Debugging and Testing: Proficiency in debugging React applications and writing unit tests using libraries like Jest and React Testing Library.

- **Education:**
  - Bachelor's or equivalent work experience
- **Certifications:**
  - AWS Certified Solutions Architect Associate
- **Required Experience:**
  - Minimum of 6 years of experience working with TypeScript/JavaScript, CSS, SASS, HTML, Node.js, Github, and React.js (or other JavaScript frameworks).
  - Minimum of 4 years of experience working with AWS, infrastructure as code (Terraform, CloudFormation, etc.), CI/CD pipelines (GitHub Actions, CircleCI, etc.), containerization (Docker, Kubernetes, etc.), and scripting (Python, Bash, etc.).

CLIN 04-11 – Web Developer
CLIN 04-28 – Web Developer

Full-Stack Developer with limited experience in TypeScript, Node.js, React.js, Python, CSS, SASS, and AWS Services.

- **Technology Knowledge**: maintain knowledge and skills on existing and emerging agile best practices, technologies relevant to supported projects, security best practices, etc.
- Skills & Qualifications:
  - **JavaScript/TypeScript**: Experience and proficiency in JavaScript and/or TypeScript.
  - **React.js:** Working knowledge of React.js library for building user interfaces and Single Page Applications (SPAs).
  - **Next.**js: Working knowledge of Next.js library for building web applications with React.js and Node.js.
  - **HTML/CSS**: Working knowledge of HTML and CSS for structuring and styling web pages.

    - **Node.js:** Familiarity with Node.js for building server-side applications and handling dependencies with tools like npm or yarn.
    - **Version Control**: Experience with version control systems like Git for collaborative development and managing codebase changes.
    - **AWS Services**: Familiarity with core AWS services such as:
        - **AWS Lambda** for serverless functions
        - **AWS S3** for storage
        - **AWS EC2** for virtual servers
    - **API Integration:** Ability to integrate RESTful APIs endpoints with the React frontend to fetch and manipulate data.
    - **Debugging and Testing:** Proficiency in debugging React applications and writing unit tests using libraries like Jest and React Testing Library.
- **Education:**
    - Bachelor's or equivalent work experience
- **Required Experience:**
    - Minimum of 2 years of experience working with TypeScript/JavaScript, CSS, SASS, HTML, Node.js, Github, and React.js (or other JavaScript frameworks).
    - Minimum of 1 year of experience working with AWS, infrastructure as code (Terraform, CloudFormation, etc.), CI/CD pipelines (GitHub Actions, CircleCI, etc.), containerization (Docker, Kubernetes, etc.), and scripting (Python, Bash, etc.).

CLIN 04-12 Sr. Cloud Network Solutions Architect

Entrusted with designing, implementing, and optimizing complex cloud-based solutions to meet and exceed the business objectives of our Court and clients. Your leadership and expertise will be critical in architecting and delivering scalable, secure, and high-performance network architectures that leverage cutting-edge cloud technologies and drive innovation.

Key Responsibilities:

- Cloud Network Design, Architecture, and Implementation: Architect and implement highly available and resilient hybrid network solutions utilizing cloud platforms and on-premises infrastructure, exceeding performance, scalability, and security requirements. Provide technical leadership and guidance on cloud network design best practices.
- On-premises Infrastructure Design, Architecture, and Implementation: Architect, implement, and maintain robust on-premises network solutions, including network and low-power cabling repair, troubleshooting, and resolution of on-premises issues (e.g., Point of Sale Systems, Video Surveillance Systems, Physical Access Control Systems, Voice over IP (VoIP) Systems, network (LAN and WAN) equipment, hypervisors, servers). Provide expert-level support and guidance for on-premises infrastructure.
- Solution Delivery: Lead collaborative efforts with internal teams and stakeholders to deeply understand complex business needs and translate them into detailed technical requirements. Architect innovative network solutions, develop comprehensive end-to-end implementation plans, and oversee their successful execution.
- Cloud Security: Establish and enforce robust cloud network security postures, incorporating advanced techniques such as encryption, zero-trust access controls, and

threat intelligence. Lead risk assessments, ensure compliance with relevant regulatory requirements, and champion security best practices across the organization.

- Troubleshooting & Optimization: Proactively analyze and resolve complex network issues (on-premises and in the cloud), optimize performance through advanced tuning and monitoring techniques, and ensure maximum availability and resilience for critical cloud networks. Mentor junior engineers in troubleshooting methodologies.
- Collaboration & Support: Collaborate effectively with DevOps, NetOps, SecOps, and SysOps teams to seamlessly integrate network solutions with cloud applications and services. Provide expert-level guidance and support to these teams.
- Documentation & Best Practices: Develop and maintain comprehensive documentation of network architectures, designs, and best practices, establishing a robust knowledge base for internal teams and promoting standardized operational procedures. Contribute to the development of organizational best practices and standards.
- Continuous Learning & Innovation: Proactively research and evaluate emerging cloud networking technologies, trends, and tools. Champion the adoption of innovative solutions and drive continuous improvement in network architectures and processes. Contribute to thought leadership and knowledge sharing within the organization.

Skills & Qualifications:

- Deep understanding of cloud networking principles, including VPCs, load balancers, DNS, routing, network segmentation, and security best practices.
- Extensive hands-on experience with at least two major cloud platforms such as AWS (e.g., EC2, S3, VPC, Lambda, Transit Gateway, Direct Connect) or Azure (e.g., Virtual Networks, Azure Firewall, Azure Functions, ExpressRoute).
- Mastery of network protocols (TCP/IP, BGP, OSPF, EIGRP, etc.) and advanced network security technologies (firewalls, intrusion detection/prevention systems, VPNs, etc.).
- Demonstrable expertise in infrastructure-as-code tools such as Terraform, CloudFormation, or Ansible, with experience automating network deployments and configurations.
- Extensive practical experience with technologies like Cisco UCS-C servers, Microsoft Hyper-V, RedHat Linux, VMware vSphere, and uninterruptible power supplies.
- Advanced knowledge of environmental monitors, physical access control systems, video camera surveillance systems, intercoms, and portable network kits.
- Deep experience with VoIP systems (e.g., Polycom, Cisco Call Manager), printers, scanners, kiosks, and point-of-sale systems.
- Proficiency with Windows Server and solutions such as GitHub, Zscaler, CrowdStrike, and Security Information & Event Management (SIEM) platforms (e.g., Splunk).
- Exceptional problem-solving and troubleshooting skills, with the ability to analyze complex network issues and develop effective solutions.
- Excellent communication, presentation, and interpersonal skills, with the ability to effectively communicate technical concepts to both technical and non-technical audiences.
- Ability to lead and mentor junior engineers.
- Ability to manage tasks and priorities in a dynamic and fast-paced environment.

Certifications:

- AWS Certified Solutions Architect – Professional
- Microsoft Azure Solutions Architect Expert
- Google Cloud Certified Professional Cloud Architect
- Cisco Certified Network Professional (CCNP) or higher
- Certified Information Systems Security Professional (CISSP)

Required Experience:

- Minimum of 10 years of experience in network engineering or related roles, with a focus on cloud network architecture and implementation.
- Minimum of 7 years of experience with cloud network solutions in professional services, including design, implementation, and support.
- Demonstrated experience leading and contributing to complex cloud networking projects.
- Significant experience contributing to cloud application, automation, and hybrid networking projects.
- Deep understanding of and experience working in Agile environments.

Education:

- Bachelor's degree in computer science, Information Technology, or a related field is required. Relevant work experience may substitute for formal education.
- Master's degree in a related field is preferred.

CLIN 04-14 Jr. Cloud Network Solutions Architect

Entrusted with supporting the design, implementation, and optimization of cloud-based solutions to meet the business objectives of our Court and clients. Your contributions will be valuable in supporting scalable, secure, and high-performance network architectures that align with modern cloud technologies.

Key Responsibilities:

- Cloud Network Design, Architecture, and Implementation: Assist in the design and implementation of hybrid network solutions using cloud platforms and on-premises infrastructure, ensuring they meet performance, scalability, and security requirements. Will work under the guidance of senior architects.
- On-premises Infrastructure Design, Architecture, and Implementation: Assist in the design, implementation, and maintenance of the on-premises network solution, including network and low-power cabling repair, troubleshooting, and resolving on-premises issues (e.g., Point of Sale System, Video Surveillance System, Physical Access Control System, Voice Over IP (VoIP) System, network (LAN and WAN) equipment, hypervisor, servers). Will work under the guidance of senior architects.
- Solution Delivery: Collaborate with internal teams and stakeholders to understand basic business needs and gather technical requirements, assist in the development of network solution architectures, and support the delivery of implementation plans.

- Cloud Security: Support the implementation of cloud network infrastructure adhering to security best practices, including encryption and access controls. Contribute to basic risk assessments under the guidance of senior security personnel.
- Troubleshooting & Optimization: Assist in analyzing and troubleshooting network issues (on-premises and in the cloud), support performance optimization efforts, and ensure high availability for cloud networks.
- Collaboration & Support: Work closely with DevOps, NetOps, SecOps, and SysOps teams to integrate network solutions with cloud applications and services.
- Documentation & Best Practices: Contribute to the maintenance of documentation for network architectures, designs, and best practices to support internal knowledge sharing and operational processes.
- Continuous Learning: Actively pursue continuous learning of emerging cloud networking technologies, trends, and tools to improve solutions and processes.

Skills & Qualifications:

- Foundational understanding of cloud networking principles, including VPCs, load balancers, DNS, and routing.
- Basic hands-on experience with at least one major cloud platform such as AWS (e.g., EC2, S3, VPC, Lambda) or Azure (e.g., Virtual Networks, Azure Firewall, Azure Functions).
- Familiarity with network protocols (TCP/IP, BGP, OSPF, etc.) and basic network security technologies.
- Exposure to infrastructure-as-code tools such as Terraform, CloudFormation, or Ansible is a plus.
- Basic practical experience with technologies like Cisco UCS-C servers, Microsoft Hyper-V, RedHat Linux, and uninterruptible power supplies.
- Basic knowledge of environmental monitors, physical access control systems, video camera surveillance systems, intercoms, and portable network kits.
- Basic experience with VoIP systems (e.g., Poly phone), printers, scanners, kiosks, and point-of-sale systems.
- Familiarity with Windows Server and solutions such as GitHub, Zscaler, CrowdStrike, and Security Information & Event Management (SIEM) platforms (e.g., Splunk) is a plus.
- Developing problem-solving and troubleshooting skills.
- Developing effective communication and teamwork abilities.
- Ability to perform physical tasks such as climbing ladders, lifting moderately heavy equipment (e.g., racking equipment), and working in confined spaces.
- Ability to manage tasks and priorities in a dynamic environment.

Certifications:

- AWS Certified Solutions Architect – Associate
- Microsoft Azure Fundamentals or Associate
- CompTIA Network+ or Security+ or Server+ or Cloud+

Required Experience:

- Minimum of 2 years of experience in network engineering or related IT roles.

- Some experience with cloud network solutions is preferred.
- Experience contributing to IT projects is a plus.

Education:

- Associate or bachelor's degree in computer science, Information Technology, or a related field is preferred. Relevant work experience may substitute for formal education.

CLIN 04-15 Sr. Cloud Network Systems Engineer

A highly experienced and results-driven individual responsible for architecting, implementing, and leading the management of complex cloud infrastructure and networking solutions. This role demands deep expertise in cloud technologies, network systems, and security best practices, enabling the optimization of cloud resources, proactive management of network configurations, and seamless integration between on-premises and cloud-based systems. The Sr. Cloud Network Systems Engineer will provide technical leadership and mentorship to junior engineers.

Key Responsibilities:

- Cloud Infrastructure Architecture & Implementation: Architect, deploy, and manage highly available, scalable, and secure cloud-based network solutions that seamlessly integrate with existing on-premises infrastructure and support business objectives. Provide expert guidance on cloud architecture best practices.
- On-premises Infrastructure Strategy & Management: Develop and execute strategies for the design, implementation, and maintenance of on-premises network solutions, including network and low-power cabling, troubleshooting, and resolving on-premises issues for critical business systems (e.g., Point of Sale, Video Surveillance, Physical Access Control, VoIP, LAN/WAN equipment, hypervisors, servers). Lead the modernization and optimization of on-premises infrastructure.
- Network Configuration, Automation, and Orchestration: Design, implement, and manage advanced network configurations within cloud environments, leveraging automation and orchestration tools to ensure optimal performance, reliability, and security. Champion the adoption of Infrastructure as Code (IaC).
- Collaboration, Consultation, and Mentorship: Provide expert consultation and collaborate effectively with cloud architects, security teams, application developers, and business stakeholders to ensure cloud infrastructure aligns with business needs and security requirements. Mentor and guide junior engineers.
- Security & Compliance Leadership: Define and enforce security policies and standards within cloud networks, implementing and managing advanced security measures, including firewalls, VPNs, encryption, intrusion detection/prevention systems, and access control mechanisms. Lead security audits and compliance initiatives.
- Troubleshooting & Expert Support: Provide expert-level support for complex network-related issues in cloud environments, leading root cause analysis, implementing permanent fixes, and ensuring minimal downtime. Escalate and manage vendor support as needed.

- Monitoring, Reporting, and Optimization: Design and implement comprehensive monitoring and reporting solutions to track network performance, security posture, and resource utilization. Proactively identify and implement optimizations to enhance performance, scalability, and cost-efficiency. Develop performance dashboards and reporting.
- Capacity Planning and Performance Tuning: Forecast cloud network capacity needs and implement proactive measures to ensure scalability and performance. Lead performance tuning and optimization efforts.

Skills & Qualifications:

- Extensive practical experience with multiple cloud platforms (AWS, Microsoft Azure, GCP) and hybrid cloud environments.
- Deep understanding of cloud security best practices, including securing data transmission, access control, identity management, and compliance frameworks (NIST, ISO 27001).
- Expert knowledge of networking protocols and network security technologies (e.g., TCP/IP, DNS, BGP, OSPF, routing, firewalls, VPNs, IDS/IPS, WAF).
- Expertise in network automation and orchestration tools and scripting languages (e.g., Python, Ansible, Terraform, CloudFormation).
- Deep familiarity with cloud-specific networking services (e.g., VPC, Direct Connect, ExpressRoute, Cloud VPN, Load Balancers, Transit Gateway).
- Extensive experience with network monitoring and management tools (e.g., CloudWatch, Azure Monitor, Datadog, New Relic, Prometheus).
- Deep familiarity with Windows Server and Linux operating systems, software tools like GitHub, Zscaler, CrowdStrike, and SIEM platforms (e.g., Splunk).
- Extensive practical experience with technologies like Cisco UCS-C servers, Microsoft Hyper-V, RedHat Linux, and uninterruptible power supplies.
- Deep understanding of environmental monitors, physical access control systems, video camera surveillance systems, intercoms, and portable network kits.
- Extensive experience with VoIP systems (e.g., Poly phone), printers, scanners, kiosks, and point-of-sale systems.
- Exceptional analytical, problem-solving, and communication skills.
- Proven ability to lead and mentor technical teams.
- Ability to perform physical tasks such as climbing ladders, lifting heavy equipment, and working in confined spaces.
- Ability to manage complex projects and prioritize tasks in a dynamic environment.

Certifications:

- AWS Certified Solutions Architect – Professional
- Microsoft Azure Solutions Architect Expert
- Google Cloud Certified Professional Cloud Architect
- CompTIA Security+ or Cloud+
- Certified Information Systems Security Professional (CISSP)

Required Experience:

- Minimum of 10 years in network engineering, cloud infrastructure, or a related role, with a strong focus on cloud and hybrid environments.
- Proven track record of designing, implementing, and managing complex cloud-based and hybrid networking solutions.
- Extensive experience working with hybrid cloud environments and multi-cloud setups.
- Significant experience leading large-scale infrastructure projects or working in a DevOps or cloud engineering team.

Education:

- Bachelor's degree in computer science, Information Technology, or a related field is preferred. A Master's degree is a plus.
- Relevant work experience may substitute for formal education in exceptional circumstances.

CLIN 04-17 Jr. Cloud Network Systems Engineer

Responsible for supporting the design, implementation, and management of cloud infrastructure and networking solutions to ensure high performance, scalability, and security for the Cloud's cloud environment. This role combines developing expertise in cloud technologies with a growing understanding of network systems, assisting in optimizing cloud resources, managing network configurations, and supporting a seamless connection between on-premises and cloud-based systems.

Key Responsibilities:

- Cloud Infrastructure Design & Implementation: Assist in the design, deployment, and maintenance of cloud-based network solutions that integrate with existing on-premises infrastructure, working under the guidance of senior engineers.
- On-prem Infrastructure Design, Architecture, and Implementation: Assist in the design, implementation, and maintenance of the on-premises network solution, including network and low-power cabling repair, troubleshooting, and resolving on-premises issues (e.g., Point of Sale System, Video Surveillance System, Physical Access Control System, Voice Over IP (VoIP) System, network (LAN and WAN) equipment, hypervisor, servers), working under the guidance of senior engineers.
- Network Configuration & Management: Support the configuration, monitoring, and troubleshooting of network systems within cloud environments, contributing to optimal performance and reliability.
- Collaboration & Consultation: Collaborate with cloud architects, security teams, and other stakeholders to support the development of cloud infrastructure solutions that meet business needs.
- Automation & Optimization: Assist in the implementation of basic automation and orchestration tools to streamline network management processes and support resource optimization efforts.
- Security & Compliance: Support the implementation of security policies and standards within cloud networks, including contributing to firewalls, VPNs, and encryption measures.

- Troubleshooting & Support: Provide support for network-related issues in cloud environments, assisting in resolving technical challenges and supporting minimal downtime.
- Monitoring & Reporting: Utilize monitoring tools to track network performance and assist in the preparation of reports to management and teams on the health of cloud network infrastructure.

Skills & Qualifications:

- Basic practical experience with cloud platforms such as AWS, Microsoft Azure, or Datacenter.
- Developing knowledge of cloud security practices, including securing data transmission and access control.
- Familiarity with networking protocols and basic network security technologies (e.g., TCP/IP, DNS, routing, firewalls, VPNs, etc.).
- Exposure to network automation tools and scripting languages like Python, Ansible, or Terraform or similar is a plus.
- Familiarity with cloud-specific networking services (e.g., VPC, Direct Connect, Cloud VPN, Load Balancers, etc.) is a plus.
- Exposure to network monitoring tools.
- Familiarity with Windows Server and software tools like GitHub, Zscaler, CrowdStrike, and SIEM platforms (e.g., Splunk) is a plus.
- Basic practical experience with technologies like Cisco UCS-C servers, Microsoft Hyper-V, RedHat Linux, and uninterruptible power supplies.
- Basic knowledge of environmental monitors, physical access control systems, video camera surveillance systems, intercoms, and portable network kits.
- Basic experience with VoIP systems (e.g., Poly phone), printers, scanners, kiosks, and point-of-sale systems.
- Developing analytical, problem-solving, and communication skills.
- Developing proficiency in troubleshooting network issues, diagnosing root causes, and resolving problems effectively.
- Developing individual initiative, contribution, and collaboration abilities.
- Ability to perform physical tasks such as climbing ladders, lifting moderately heavy equipment (e.g., racking equipment), and working in confined spaces.
- Ability to manage tasks and priorities in a dynamic environment.

Certifications:

- AWS Certified – Foundational or Associate
- Microsoft Azure Certified – Fundamentals or Associate
- CompTIA Network+ or Security+ or Server+ or Cloud+

Required Experience:

- Minimum of 2 years in network engineering, IT infrastructure, or a related role.
- Some experience with cloud infrastructure is preferred.
- Experience contributing to IT projects is a plus.

Education:

- Associate or bachelor's degree in computer science, Information Technology, or a related field is preferred. Relevant work experience may substitute for formal education.

CLIN 04-18 Sr. Cloud Network Operations Administrator

A key leadership role in the proactive management, monitoring, optimization, and strategic evolution of cloud-based and hybrid network infrastructure. This individual will collaborate closely with cross-functional teams, providing expert guidance and mentorship to ensure seamless, secure, and highly performant operations of cloud network environments and services. The ideal candidate possesses extensive experience working with diverse cloud platforms (AWS, Azure, GCP), on-premises infrastructure, and advanced troubleshooting and problem-solving skills to maintain high availability, security, and performance of complex hybrid network infrastructures.

Key Responsibilities:

- Incident Management Leadership: Lead troubleshooting and resolution of complex cloud network-related incidents and issues, driving root cause analysis, implementing preventative measures, and ensuring minimal downtime and prompt service restoration. Mentor junior staff in incident management best practices.
- On-premises Infrastructure Administration & Strategy: Oversee the daily administration of on-premises systems and network appliances, including cabling, servers, hypervisors, and critical business systems (Point of Sale, Video Surveillance, Physical Access Control, VoIP, LAN/WAN equipment). Develop and implement strategies for optimizing and modernizing on-premises infrastructure.
- Performance Monitoring & Optimization: Design, implement, and analyze performance metrics for cloud and hybrid networks, proactively identifying bottlenecks and implementing optimizations to ensure optimal performance, scalability, and efficiency. Develop performance dashboards and reporting.
- Automation & Orchestration: Architect, develop, and maintain advanced automation and orchestration scripts to streamline cloud network provisioning, configuration, monitoring, and lifecycle management processes. Champion the adoption of Infrastructure as Code (IaC) principles.
- Security & Compliance Leadership: Collaborate with security teams to define and enforce cloud network security best practices and compliance standards. Provide expert guidance on security hardening, vulnerability management, and audit readiness.
- Documentation & Knowledge Management: Establish and maintain comprehensive documentation for network configurations, processes, procedures, and best practices related to cloud and hybrid network operations. Foster a culture of knowledge sharing and documentation excellence.
- Collaboration & Strategic Partnership: Collaborate strategically with other IT teams, cloud architects, developers, and business stakeholders to integrate cloud network solutions into broader infrastructure strategies and business objectives. Provide expert guidance on cloud network architecture and design.

- Cloud Network Deployment Enablement: Lead the planning, deployment, and migration of complex cloud-based network solutions and services for new and ongoing projects. Provide technical leadership and guidance to project teams.
- Troubleshooting & Expert Support: Provide expert-level support for complex operational issues within the cloud and hybrid network infrastructure, ensuring continuity of service for business-critical applications. Escalate and manage vendor support as needed.

Skills & Qualifications:

- Proficient in network operations and system operations, with a strong focus on hybrid and cloud network environments.
- Extensive hands-on experience with multiple cloud platforms (AWS, Azure, GCP) and related services.
- Deep understanding of hybrid network infrastructure and related services.
- Deep understanding of on-premises network infrastructure and related services.
- Expert proficiency in network protocols (TCP/IP, DNS, HTTP/HTTPS, BGP, OSPF, etc.) and security technologies (Firewall, VPNs, IDS/IPS, WAF).
- Extensive experience with advanced monitoring and cloud infrastructure management tools (e.g., CloudWatch, Azure Monitor, Prometheus, Datadog, New Relic).
- Expertise in automation and scripting languages (e.g., Python, PowerShell, Terraform, Ansible).
- Deep knowledge of security best practices, frameworks (NIST, ISO 27001), and tools.
- Exceptional troubleshooting and problem-solving skills, including root cause analysis methodologies.
- Strong leadership, communication, and collaboration skills, with the ability to mentor and guide junior staff.
- Expert understanding of networking concepts such as VPN, SD-WAN, DNS, and network segmentation.
- Ability to perform physical tasks such as climbing ladders, lifting heavy equipment, and working in confined spaces.

Certifications:

- AWS Certified Solutions Architect – Professional
- Microsoft Azure Network Engineer Expert
- Google Cloud Certified Professional Cloud Architect
- CompTIA Certified – Network+, Security+, Server+, Cloud+
- ITIL Expert Certification

Required Experience:

- Minimum of 10 years of experience in network engineering or network operations, with a focus on cloud and hybrid environments.
- Extensive experience with containerization and microservices networking (Kubernetes, Docker).
- Proven experience designing, implementing, and managing hybrid cloud and multi-cloud network environments.
- Extensive hands-on experience with cloud platforms (AWS, Azure, GCP) and related networking services.

- Extensive hands-on experience with hybrid network infrastructure and related networking services.
- Extensive hands-on experience with on-premises network infrastructure and related networking services.
- Proven experience with cloud-based and hybrid network troubleshooting, performance optimization, and security hardening.
- Significant experience in managing complex hybrid or multi-cloud network environments.
- Expertise in network automation and orchestration tools and frameworks.

Education:

- Bachelor's degree in computer science, Information Technology, or a related field is preferred. A Master's degree is a plus.
- Relevant work experience may substitute for formal education in exceptional circumstances.

CLIN 04-20 Jr. Cloud Network Operations Administrator

A key role in supporting the management, monitoring, and optimization of cloud-based network infrastructure. This individual will work closely with cross-functional teams to ensure seamless operations of cloud network environments and services. The ideal candidate will have some experience working with cloud platforms such as AWS, Azure, and on-premises infrastructure, and will possess developing troubleshooting and problem-solving skills to maintain high availability, security, and performance of hybrid network infrastructures.

Key Responsibilities:

- Incident Management: Assist in troubleshooting and resolving cloud network-related incidents and issues, ensuring minimal downtime and prompt service restoration. Will work under the guidance of senior administrators.
- Administration of On-prem Infrastructure: Assist in the daily administration of on-premises systems and network appliances, including cabling, servers, hypervisor, Point of Sale System, Video Surveillance System, Physical Access Control System, Voice Over IP (VoIP) System, and network (LAN and WAN) equipment. Will work under the guidance of senior administrators.
- Performance Monitoring: Support the implementation and monitoring of performance metrics for cloud networks, ensuring optimal performance, scalability, and efficiency.
- Automation & Scripting: Assist in the development and maintenance of automation scripts to streamline cloud network provisioning, configuration, and monitoring processes.
- Security and Compliance: Support security teams to ensure the cloud network architecture adheres to security best practices and compliance standards.
- Documentation: Contribute to the maintenance of documentation for network configurations, processes, and procedures related to cloud network operations.
- Collaboration: Work collaboratively with other IT teams, cloud architects, and developers to integrate cloud network solutions into broader infrastructure strategies.

- Support Cloud Network Deployments: Assist in the planning and deployment of cloud-based network solutions and services for new and ongoing projects.
- Troubleshooting and Support: Provide first-level support for day-to-day operational issues within the cloud network infrastructure, ensuring continuity of service for business-critical applications.

Skills & Qualifications:

- Proficient in network operations or related IT roles.
- Some experience with cloud platforms (AWS, Azure) and related services is preferred.
- Some experience with hybrid network infrastructure and related services is preferred.
- Some experience with on-premises network infrastructure and related services is preferred.
- Basic understanding of network protocols (TCP/IP, DNS, HTTP/HTTPS, etc.) and security technologies (Firewall, VPNs).
- Familiarity with monitoring tools and cloud infrastructure management (e.g., CloudWatch, Azure Monitor) is a plus.
- Exposure to automation and scripting tools (e.g., Python, PowerShell, Terraform) is a plus.
- Basic knowledge of security best practices and tools.
- Developing troubleshooting skills.
- Ability to perform physical tasks such as climbing ladders, lifting moderately heavy equipment (e.g., racking equipment), and working in confined spaces.
- Developing strong communication skills and ability to collaborate with multiple teams.
- Basic understanding of networking concepts such as VPN, SD-WAN, and DNS.

Certifications:

- AWS Certified Solutions Architect – Associate or Cloud Practitioner
- Microsoft Azure Fundamentals or Associate
- CompTIA Network+ or Security+ or Cloud+
- ITIL Foundation Certification

Required Experience:

- Minimum of 2 years of experience in network engineering or network operations, or related IT roles.
- Familiarity with cloud platforms (AWS, Azure) and related networking services is a plus.
- Familiarity with hybrid network infrastructure and related networking services is a plus.
- Familiarity with on-premises network infrastructure and related networking services is a plus.
- Experience with network troubleshooting is a plus.

Education:

- Associate or bachelor's degree in computer science, Information Technology, or a related field is preferred.
- Relevant work experience may substitute for formal education.

CLIN 04-29 Business Process Engineer

The Business Process Engineer (BPE) is responsible for analyzing, designing, and improving the Court's processes to enhance operational efficiency and effectiveness. This role involves working closely with stakeholders to identify bottlenecks, optimize workflows, and implement process automation solutions. A BPE is expected to have a strong understanding of business process methodologies and technology solutions, balancing technical expertise with process improvement strategies.

Key Responsibilities:

Process Analysis & Optimization:

- Evaluate existing business processes to identify inefficiencies and areas for improvement.
- Conduct root cause analysis and recommend solutions to streamline workflows.
- Develop process maps, workflows, and documentation to support process redesign efforts.

Process Design & Implementation:

- Collaborate with business and IT teams to design scalable and sustainable process improvements.
- Utilize Lean, Six Sigma, or BPM (Business Process Management) methodologies to drive process optimization.
- Ensure that process changes align with business objectives, regulatory requirements, and industry best practices.

Technology & Automation Integration:

- Work with IT teams to implement process automation tools, including RPA (Robotic Process Automation) and BPM software.
- Support the integration of process improvements with ERP, CRM, or workflow management systems.
- Identify opportunities for AI and data analytics to enhance decision-making and operational efficiency.

Stakeholder Collaboration & Change Management:

- Engage with business units to gather requirements and ensure process improvements meet organizational needs.
- Facilitate workshops and training sessions to help teams adopt new processes.
- Support change management initiatives by communicating process changes effectively across departments.

Performance Measurement & Continuous Improvement:

- Define and track key performance indicators (KPIs) to measure process effectiveness.
- Conduct post-implementation reviews to assess the impact of process improvements.
- Promote a culture of continuous improvement by recommending iterative enhancements.

Skills & Qualifications:

- Strong understanding of business process modeling, workflow automation, and process improvement methodologies.
- Proficiency in BPM tools such as Visio, Bizagi, ARIS, or similar platforms.
- Knowledge of process automation technologies, including RPA tools (e.g., UiPath, Blue Prism, Automation Anywhere).
- Familiarity with Agile, Lean, or Six Sigma methodologies for process improvement.
- Ability to analyze business requirements and translate them into technical solutions.
- Experience with data analysis and performance tracking using Excel, Power BI, or similar tools.
- Strong problem-solving skills and the ability to identify root causes of process inefficiencies.
- Excellent communication and stakeholder management skills to engage cross-functional teams.
- Ability to document workflows, SOPs, and process diagrams for training and compliance.

Certifications:

- Lean Six Sigma Green Belt or Black Belt
- Certified Business Process Professional (CBPP)
- Agile Business Analyst (IIBA-AAC)
- Project Management Professional (PMP) or Certified Scrum Master (CSM)
- Business Process Management Certification (BPMN, BPMP, or equivalent)
- Robotic Process Automation (RPA) Certifications (UiPath, Automation Anywhere, or Blue Prism)

Required Experience:

- Minimum of 5 years of experience in business process analysis, process engineering, or related fields.
- Hands-on experience with process mapping and workflow automation tools.
- Exposure to working with enterprise systems (ERP, CRM, or BPM platforms).
- Experience in cross-functional collaboration within IT and business teams.
- Previous involvement in process improvement initiatives with measurable impact.

CLIN 04-30 Data Architect

The Data Architect is responsible for designing, implementing, and managing data architectures that support business intelligence, analytics, and operational applications. This role ensures the integrity, scalability, and security of data systems while optimizing data flow and storage across the organization. A mid-tier Data Architect is expected to collaborate with cross-functional teams to define data strategies, enforce best practices, and support data-driven decision-making.

Key Responsibilities:
Data Architecture & Design:

- Develop and maintain data models, database schemas, and data flow diagrams.
- Ensure data architecture aligns with business goals, scalability needs, and compliance requirements.
- Optimize data storage and retrieval processes for performance and cost efficiency.

Data Integration & Management:

- Design and oversee ETL (Extract, Transform, Load) processes to ensure efficient data movement.
- Implement data pipelines to support analytics, reporting, and machine learning workloads.
- Ensure data quality, consistency, and governance across multiple sources.

Database & Cloud Solutions:

- Work with relational and NoSQL databases, including SQL Server, PostgreSQL, MongoDB, and Cassandra.
- Support cloud-based data platforms such as AWS Redshift, Google BigQuery, and Azure Synapse.
- Implement data lake and data warehouse architectures to support large-scale data storage and analytics.

Security, Compliance & Governance:

- Implement data security best practices, including encryption, access control, and auditing.
- Ensure compliance with data regulations such as GDPR, CCPA, and HIPAA.
- Define and enforce data governance policies, metadata management, and lineage tracking.

Collaboration & Stakeholder Engagement:

- Work closely with data engineers, analysts, and business stakeholders to understand data requirements.
- Provide guidance on best practices for database development and data integration.
- Support IT and business teams in adopting new data technologies and solutions.

Skills & Qualifications:

- Strong understanding of data modeling, relational and NoSQL database design, and data architecture principles.
- Proficiency in SQL and database optimization techniques.
- Experience with ETL tools such as Apache NiFi, Talend, or Informatica.
- Familiarity with big data technologies, including Hadoop, Spark, and Kafka.
- Knowledge of cloud-based data platforms (AWS, Azure, GCP) and their data services.
- Understanding of data governance, metadata management, and data security best practices.
- Ability to work with APIs, microservices, and real-time data streaming solutions.
- Strong analytical, troubleshooting, and problem-solving skills.
- Effective communication skills to translate business needs into technical solutions.

Certifications:

- AWS Certified Data Analytics – Specialty or current equivalent
- Microsoft Certified: Azure Data Engineer Associate or current equivalent

- DAMA Certified Data Management Professional (CDMP)

Required Experience:

- Minimum of 5 years of experience in data architecture, data engineering, or database management.
- Hands-on experience with designing and implementing large-scale data solutions.
- Familiarity with data lakes, warehouses, and real-time analytics frameworks.
- Prior work with cloud-based data solutions and enterprise data management.
- Experience in collaborating with cross-functional teams on data governance and security initiatives.

CLIN 04-31 Data Engineer

The Data Engineer plays a pivotal role in managing and optimizing data pipelines, data warehousing, and ensuring the integrity of the Court's data infrastructure. This role requires the ability to design, implement, and maintain systems that allow data to flow seamlessly across various sources and platforms. As a key player in the team, the individual will collaborate closely with data scientists, analysts, and Court personnel to ensure the efficient and secure handling of data.

Key Responsibilities:

- API Design, Development, and Maintenance: Design, build, and maintain APIs to enable efficient data sharing between systems, ensuring proper documentation, security, and scalability of API solutions. Data Pipeline Development: Design, build, and maintain scalable and efficient data pipelines for ingesting, processing, and storing large volumes of structured and unstructured data.
- Data Modeling and Data Dictionary: Work with stakeholders to create data models that support business needs and improve the usability of data across the organization.
- Data Warehousing: Manage and optimize the Court's data warehouse(s), ensuring data accuracy and accessibility for analytics and reporting.
- ETL Processes: Develop and maintain Extract, Transform, Load (ETL) processes to integrate data from various sources into centralized repositories.
- Data Quality Assurance: Ensure high data quality standards through automated tests, validation checks, and monitoring systems.
- Collaboration: Work alongside data scientists, analysts, and business teams to understand data needs, translate business requirements into technical specifications, and support data-driven decision-making.

Skills & Qualifications:

- Proficient in Programming Languages: Strong experience with languages such as Python, SQL, Java, or Scala for data manipulation, processing, and automation.
- Data Modeling and Databases: Expertise in relational databases (e.g., PostgreSQL, MySQL) and experience with NoSQL databases (e.g., MongoDB, Cassandra).
- ETL Tools and Frameworks: Knowledge of ETL tools such as Apache NiFi, Talend, or Airflow for managing data workflows.

- Cloud Platforms: Familiarity with cloud-based data engineering solutions such as AWS or Azure, including services like AWS Redshift and Azure Data Factory.
- Version Control: Experience with version control systems such as Git for managing code and collaboration.
- Data Warehousing and Business Intelligence: Strong understanding of data warehousing concepts and BI tools like Tableau, Power BI, or Looker.
- Problem Solving and Analytical Skills: Ability to analyze complex data problems and propose effective solutions in a collaborative environment.

Certifications:

- AWS Certified Big Data - Specialty: Validates expertise in designing and implementing big data solutions on AWS.
- Microsoft Certified: Azure Data Engineer Associate: Confirms expertise in implementing and managing data solutions on Microsoft Azure.

Required Experience:

- Professional Experience: Minimum of 5 years of experience in a data engineering role or similar technical position focused on data pipelines, data integration, and cloud-based solutions.
- Project Experience: Hands-on experience with end-to-end data engineering processes, including data extraction, transformation, loading, and storage.
- Collaborative Experience: Proven track record of working in cross-functional teams, collaborating with data scientists, analysts, and business units to meet data requirements and optimize systems.
- Tool Familiarity: Experience with popular data engineering tools and frameworks, such as Apache Hadoop, Spark, Kafka, and Data Build Tools (dbt), is highly beneficial.

CLIN 04-32 Data Scientist

The Data Scientist is responsible for applying analytical and machine learning techniques to interpret complex data, generate insights, and guide business decisions. This role requires the ability to work with large datasets, develop predictive models, and communicate findings effectively to both technical and non-technical stakeholders. The ideal candidate should possess a strong background in statistics, programming, and data analysis, and be able to take ownership of data-driven projects from start to finish. As a key member of the data science team, the individual will collaborate with data engineers, business analysts, and product teams to address business challenges using data-driven solutions.

Key Responsibilities:

- Data Analysis & Exploration: Conduct exploratory data analysis (EDA) to uncover trends, patterns, and relationships within large datasets, ensuring data quality and identifying areas for improvement.
- Model Development & Deployment: Develop and implement machine learning models, including classification, regression, and clustering, for predictive analytics, anomaly detection, and decision-making support.

- Feature Engineering: Design and create features from raw data to enhance model performance, ensuring the data is structured appropriately for analysis and modeling.
- Statistical Analysis: Apply statistical methods to analyze data and validate model outcomes, providing actionable insights based on data.
- Collaboration & Reporting: Work closely with cross-functional teams (e.g., data engineers, product managers, business analysts) to understand business problems, provide data-driven solutions, and present findings in a clear and actionable manner.
- Model Evaluation & Optimization: Evaluate the performance of models using appropriate metrics and optimize models for accuracy, speed, and scalability.

Skills & Qualifications:

- Programming Languages: Proficiency in Python, R, or similar programming languages commonly used for data analysis and machine learning.
- Machine Learning & Statistical Techniques: Strong knowledge of machine learning algorithms (e.g., decision trees, SVMs, neural networks) and statistical methods (e.g., hypothesis testing, A/B testing).
- Data Wrangling: Expertise in cleaning, transforming, and manipulating large datasets using tools like pandas, NumPy, or similar libraries.
- Data Visualization: Experience with data visualization tools (e.g., Matplotlib, Seaborn, Plotly) to present data and model results in a clear, understandable format.
- Big Data & Cloud Platforms: Familiarity with working on big data platforms (e.g., Hadoop, Spark) and cloud services (e.g., AWS, Azure) for scalable data analysis.
- Database Knowledge: Proficiency in SQL for querying relational databases and extracting data for analysis.

Certifications:

- Certified Data Scientist (Data Science Council of America - DASCA): A certification that validates expertise in applying data science techniques in a professional environment.
- AWS Certified Machine Learning - Specialty: Demonstrates knowledge and skills in machine learning, artificial intelligence, and deep learning using AWS cloud technologies.
- Microsoft Certified: Azure Data Scientist Associate: Indicates expertise in data science practices, machine learning, and data analysis within the Azure environment.

Required Experience:

- Professional Experience: Minimum of 7 years of experience working as a data scientist or in a similar role focused on data analysis, machine learning, and statistical modeling.
- Project Experience: Experience in developing end-to-end data science projects, from problem definition and data collection to model development and deployment.
- Collaboration Experience: Proven ability to work with cross-functional teams, including business stakeholders, data engineers, and product teams, to solve complex business problems using data science techniques.
- Machine Learning & Deployment: Hands-on experience with deploying machine learning models into production environments and maintaining models' post-deployment.

- Advanced Analytical Techniques: Experience with advanced analytics techniques, including deep learning, natural language processing (NLP), and time series forecasting, is a plus.

H4.4 Cybersecurity Segment LCAT Descriptions

CLIN 05-01 – Information System Support Officer (ISSO)
CLIN 05-05 – Information System Support Officer (ISSO)

Responsible for maintaining the appropriate operational security posture for the Court's information systems. The ISSO works in close collaboration with the Information System owner, Information System Security Manager (SSM), and management official to ensure a proper security posture is in place.

Key Responsibilities:

Security Assessment & Monitoring:

- Conduct regular security assessments and audits of information systems to identify and mitigate vulnerabilities.
- Monitor system activity for security incidents and anomalies.
- Analyze security logs and identify suspicious activity.
- Implement and maintain security controls, such as firewalls, intrusion detection systems, and antivirus software.

Security Policy & Compliance:

- Develop, implement, and maintain security policies, procedures, and standards for information systems.
- Ensure compliance with relevant security regulations and standards (e.g., NIST, ISO 27001, HIPAA).
- Provide guidance and training to users on security policies and procedures.

Risk Management:

- Conduct risk assessments to identify and evaluate potential threats and vulnerabilities.
- Develop and implement risk mitigation strategies.
- Maintain and update risk assessments on an ongoing basis.

Incident Response:

- Develop and maintain incident response plans.
- Investigate security incidents, collect and analyze evidence, and assist in the remediation process.
- Coordinate incident response activities with other relevant personnel (e.g., IT staff, legal counsel).

Communication & Collaboration:

- Communicate security issues and concerns to management and stakeholders.
- Collaborate with other ISSOs and security professionals to share best practices and lessons learned.
- Maintain effective communication with system owners and users.

Skills & Qualifications:

- Strong understanding of cybersecurity principles and best practices: Familiarity with common attack vectors, security frameworks, and regulatory compliance requirements.
- Knowledge of information systems and technologies: Understanding of operating systems, databases, networks, and other IT infrastructure components.

- Risk management and assessment skills: Ability to identify, assess, and mitigate security risks.
- Analytical and problem-solving skills: Ability to analyze security issues, identify root causes, and develop effective solutions.
- Excellent communication and interpersonal skills: Ability to communicate technical information clearly and concisely to both technical and non-technical audiences.
- Strong attention to detail and organizational skills: Ability to manage multiple tasks, prioritize effectively, and work independently.

Certifications:

- CompTIA Security+: A foundational certification demonstrating a broad understanding of cybersecurity concepts and principles.
- Certified Information Systems Security Professional (CISSP): A globally recognized certification for information security professionals.
- GIAC certifications: A range of certifications offered by the GIAC (Global Information Assurance Certification) organization covering specific areas of cybersecurity (e.g., GCIH, GPEN, GCIA).
- Relevant industry-specific certifications: For example, certifications related to specific technologies or regulatory compliance requirements.

Required Experience:

- Minimum of 7 years of experience in an ISSO or equivalent role or a related cybersecurity field.
- Experience with security tools and technologies such as firewalls, Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Endpoint Detection & Response (EDR), Zero Trust Security (ZTS), Data Loss Prevention (DLP), Security Information & Event Management (SIEM), vulnerability solutions & penetration testing.
- Experience with incident response and security investigations.
- Experience with risk management and compliance frameworks.

CLIN 05-02 Cybersecurity Engineer
CLIN 05-08 Cybersecurity Engineer

Plays a crucial role in safeguarding the Court's digital assets by designing, implementing, and maintaining robust security measures. Responsible for identifying and mitigating cyber threats, ensuring the confidentiality, integrity, and availability of sensitive data and systems.

Key Responsibilities:

Conducting Security Assessments & Penetration Testing:

- Perform vulnerability assessments using various tools and techniques (e.g., network scanning, code reviews, penetration testing) to identify and document security weaknesses.
- Conduct penetration testing to simulate real-world attacks and evaluate the effectiveness of existing security controls.
- Analyze security logs and identify suspicious activity.

- Generate comprehensive reports detailing findings, risks, and remediation recommendations.

Implementing & Managing Security Controls:

- Design, deploy, and configure security controls such as firewalls, Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Endpoint Detection & Response (EDR), Zero Trust Security (ZTS), Security Information & Event Management (SIEM) solutions.
- Monitor security systems for alerts and anomalies, investigate security incidents, and respond to security breaches effectively.
- Manage security access controls, including user authentication, authorization, and access rights.
- Implement and maintain security policies, procedures, and standards.

Incident Response & Forensics:

- Develop and maintain incident response plans.
- Investigate security incidents, collect and analyze evidence, and assist in the remediation process.
- Conduct forensic analysis of systems and data to identify the root cause of security breaches.

Staying Current on Threats & Technologies:

- Research and stay updated on emerging cyber threats, vulnerabilities, and attack vectors.
- Attend industry conferences, training sessions, and read security publications to enhance knowledge and skills.
- Evaluate and recommend new security technologies and solutions to improve the Court's security posture.

Skills & Qualifications:

- Strong understanding of cybersecurity principles and best practices: Familiarity with common attack vectors (e.g., malware, phishing, social engineering), security frameworks (e.g., NIST Cybersecurity Framework, ISO 27001), and regulatory compliance requirements (e.g., GDPR, HIPAA).
- Proficiency in network security concepts: Deep understanding of network protocols (TCP/IP, UDP, DNS), network topologies, and network devices (routers, switches, firewalls).
- Technical expertise: Proficiency in scripting languages (e.g., Python, PowerShell), command-line interfaces (CLI), and various operating systems (Windows, Linux, macOS).
- Analytical and problem-solving skills: Ability to analyze complex security issues, identify root causes, and develop effective solutions.
- Excellent communication and interpersonal skills: Ability to communicate technical information clearly and concisely to both technical and non-technical audiences.
- Strong attention to detail and organizational skills: Ability to manage multiple tasks, prioritize effectively, and work independently.

Certifications:

- CompTIA Security+: A foundational certification demonstrating a broad understanding of cybersecurity concepts and principles.
- AWS Certified Security Specialty
- Microsoft Azure Security Technologies Certified
- Certified from Zscaler, CrowdStrike, or/and Splunk vendor programs....
- Certified Ethical Hacker (CEH): A certification focusing on the technical skills required to perform ethical hacking and penetration testing.
- Certified Information Systems Security Professional (CISSP): A globally recognized certification for information security professionals.
- GIAC certifications: A range of certifications offered by the GIAC (Global Information Assurance Certification) organization covering specific areas of cybersecurity (e.g., GCIH, GPEN, GCIA).

Required Experience:

- Minimum of 7 years of professional experience in cybersecurity or a related field (e.g., systems administration, network engineering).
- Hands-on experience with security tools and technologies such as firewalls, Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Endpoint Detection & Response (EDR), Zero Trust Security (ZTS), Data Loss Prevention (DLP), Security Information & Event Management (SIEM), vulnerability assessment solutions.
- Experience with incident response and security investigations.

CLIN 05-03 Senior Cybersecurity Analyst
CLIN 05-10 Senior Cybersecurity Analyst

A highly experienced and results-oriented cybersecurity professional, the Senior Cybersecurity Analyst leads in the proactive defense of the organization's information systems. This role provides expert-level guidance on cybersecurity operations, risk mitigation, incident response, and security architecture, ensuring the organization's IT environment remains secure, resilient, and compliant with applicable regulations and standards. The Senior Analyst acts as a mentor and technical authority, driving continuous improvement in security practices and fostering a strong security culture.

Key Responsibilities:

Security Operations & Architecture:

- Architect, implement, and manage advanced security solutions, including SIEM, ZTS, EDR, IDS/IPS, and other cyber management platforms, optimizing their effectiveness and integration.
- Lead proactive threat hunting and vulnerability assessments, identifying and mitigating emerging threats before they can impact the organization.
- Develop and champion security best practices and standards, ensuring their consistent application across the organization.
- Provide expert guidance on secure system design and architecture, influencing IT projects and initiatives to incorporate security from inception.

Incident Response Leadership:

- Lead and coordinate complex incident response efforts, effectively containing and eradicating threats, minimizing business impact, and conducting thorough post-incident analysis.
- Develop and maintain comprehensive incident response plans, playbooks, and procedures, ensuring their alignment with industry best practices and regulatory requirements.
- Mentor and train junior analysts in incident response techniques, fostering their development and expertise.

Risk Management & Compliance:

- Conduct comprehensive risk assessments, identifying vulnerabilities and recommending appropriate mitigation strategies.
- Lead the development and implementation of security policies, standards, and procedures, ensuring compliance with frameworks such as NIST, ISO 27001, and other relevant regulations.
- Provide expert advice on security compliance and audit requirements, supporting internal and external audits.

Security Awareness & Training:

- Develop and deliver engaging security awareness training programs, educating employees on best practices and promoting a strong security culture.
- Mentor and guide IT staff on secure configurations and best practices, fostering their understanding of security principles.

Collaboration & Communication:

- Collaborate effectively with senior management, IT teams, and business stakeholders to communicate security risks and recommendations.
- Provide clear and concise reports on security incidents, risk assessments, and vulnerabilities, presenting complex technical information in an accessible manner.
- Represent the organization in security-related discussions with external vendors, partners, and industry groups.

Continuous Improvement & Innovation:

- Research and evaluate emerging security technologies and threats, recommending and implementing innovative solutions to enhance the organization's security posture.
- Identify process gaps and recommend enhancements to security operations, driving continuous improvement in security practices.
- Contribute to the development of the organization's overall cybersecurity strategy.

Skills & Qualifications:

Technical Expertise:

- Deep expertise in security tools and technologies, including firewalls, SIEM, IDS/IPS, ZTS, EDR, vulnerability scanning solutions, and cloud security platforms.
- Advanced understanding of network protocols, operating systems (Windows, macOS, Linux, iOS, Android), cloud environments (AWS, Azure, GCP), and containerization technologies.
- Proficiency in scripting languages (e.g., Python, PowerShell) for automation and security tasks.
- Experience with security architecture and design principles.

Analytical & Problem-Solving Skills:

- Exceptional analytical and problem-solving skills, with the ability to analyze complex security logs and events to identify patterns and potential threats.
- Proven ability to lead and manage complex security incidents.

Communication & Leadership:

- Excellent written and verbal communication skills, with the ability to effectively convey technical information to both technical and non-technical audiences.
- Demonstrated leadership skills, with the ability to mentor and guide junior analysts.

Certifications:

- CISSP (Certified Information Systems Security Professional)
- CompTIA Security+
- AWS Certified Security Specialty
- Microsoft Azure Security Technologies Certified
- Vendor certifications from leading security vendors (e.g., Zscaler, CrowdStrike, Splunk)
- Certified Ethical Hacker (CEH)
- GIAC certifications (e.g., GSEC, GCIA, GCSH)

Required Experience:

- Minimum of 10 years of hands-on experience in cybersecurity or related IT roles, with a focus on security operations, incident response, and risk management.
- Extensive experience with security monitoring tools and incident response processes.
- Deep understanding of compliance requirements and risk management frameworks such as NIST, ISO 27001, and HIPAA.
- Experience in a leadership or mentorship role.

CLIN 05-04 – Sr. Information System Support Officer (ISSO)

Leads the maintenance and enhancement of the operational security posture for the Court's information systems. The Senior ISSO strategically collaborates with Information System Owners, the Information System Security Manager (SSM), and senior management to ensure a robust and proactive security posture. Mentors and guides other security personnel.

Key Responsibilities:

Security Assessment & Monitoring:

- Develops and implements comprehensive security assessment and audit strategies for complex information systems, proactively identifying and mitigating vulnerabilities.
- Oversees the continuous monitoring of system activity for security incidents and anomalies, utilizing advanced threat intelligence and analytics.
- Expertly analyzes security logs and identifies subtle indicators of compromise, escalating critical issues as needed.
- Architects and oversees the implementation and maintenance of advanced security controls, including next-generation firewalls, intrusion detection/prevention systems, advanced endpoint protection, and security automation tools.

Security Policy & Compliance:

- Leads the development, implementation, and refinement of security policies, procedures, and standards for enterprise-level information systems, ensuring alignment with best practices and regulatory requirements.
- Drives compliance with relevant security regulations and standards (e.g., NIST, ISO 27001, HIPAA, PCI DSS), anticipating evolving regulatory landscapes.
- Provides expert guidance and training to users and other security personnel on complex security policies and procedures. • Risk Management: o Conducts enterprise-level risk assessments, employing advanced methodologies to identify and evaluate complex threats and vulnerabilities.
- Develops and champions comprehensive risk mitigation strategies, prioritizing and allocating resources effectively.
- Maintains and proactively updates risk assessments, adapting to dynamic threat landscapes.

Incident Response:

- Develops and champions enterprise-level incident response plans, incorporating advanced incident handling techniques.
- Leads complex security incident investigations, expertly collecting and analyzing evidence, and directing the remediation process.
- Coordinates incident response activities with internal teams, external partners, and legal counsel, ensuring minimal disruption and effective communication. • Communication & Collaboration: o Communicates security issues and concerns to executive management and key stakeholders, providing clear and concise risk assessments and recommendations.
- Collaborates effectively with other senior ISSOs and security professionals to share threat intelligence, best practices, and lessons learned.
- Fosters strong relationships with system owners, users, and vendors, promoting a security-conscious culture.

Skills & Qualifications:

- Deep understanding of cybersecurity principles and best practices: Expert knowledge of advanced attack vectors, security frameworks, and regulatory compliance requirements.
- Extensive knowledge of information systems and technologies: Mastery of operating systems, databases, networks, cloud platforms, and other complex IT infrastructure components.
- Advanced risk management and assessment skills: Ability to identify, assess, and mitigate complex security risks at the enterprise level.
- Exceptional analytical and problem-solving skills: Ability to analyze complex security issues, identify root causes, and develop innovative solutions.
- Excellent communication and interpersonal skills: Ability to communicate technical information clearly and persuasively to executive leadership and diverse audiences.
- Strong leadership, mentoring, and organizational skills: Ability to manage multiple complex projects, prioritize effectively, and guide other security professionals.

Certifications:

- Certified Information Systems Security Professional (CISSP): A globally recognized certification for senior information security professionals.
- GIAC certifications: Advanced certifications offered by the GIAC (Global Information Assurance Certification) organization covering specialized areas of cybersecurity (e.g., GSE, CISSP-ISSAP, CISSP-ISSEP).
- Certified Cloud Security Professional (CCSP): Demonstrates expertise in cloud security architecture, design, implementation, operations, and service orchestration.
- Relevant industry-specific certifications: For example, certifications related to specific technologies or regulatory compliance requirements.

Required Experience:

- Minimum of 10 years of progressive experience in an ISSO or equivalent role, with demonstrated leadership in cybersecurity.
- Extensive experience with security tools and technologies such as advanced security information and event management (SIEM) platforms, SOAR, threat intelligence platforms, and cloud security solutions.
- Proven experience leading complex incident response and security investigations, including forensic analysis.
- Demonstrated experience developing and implementing enterprise-level risk management and compliance frameworks.
- Experience mentoring and guiding other security professionals.

CLIN 05-06 - Jr. Information System Security Officer

Responsible for assisting in maintaining the appropriate operational security posture for the Court's information systems. The Junior ISSO works under the guidance of senior security staff and in collaboration with the Information System Owner, Information System Security Manager (SSM), and management officials to support security initiatives.

Key Responsibilities:

Security Assessment & Monitoring:

- Assist in conducting basic security assessments and audits of information systems to identify potential vulnerabilities.
- Monitor system activity for security incidents and anomalies under supervision.
- Review security logs and escalate suspicious activity to senior security personnel.
- Support the implementation and maintenance of security controls, such as firewalls and antivirus software.

Security Policy & Compliance:

- Assist in implementing and maintaining security policies, procedures, and standards.
- Ensure awareness of and adherence to relevant security regulations and standards (e.g., NIST, ISO 27001, HIPAA).
- Support training efforts by helping to educate users on security best practices.

Risk Management:

- Assist in identifying potential threats and vulnerabilities in collaboration with senior security staff.

- Help document risk assessments and mitigation strategies.
- Maintain and update risk assessment documentation as directed.

Incident Response:

- Assist in developing and maintaining incident response plans.
- Participate in investigations of security incidents, collecting and analyzing evidence under supervision.
- Support coordination of incident response activities with IT staff and security personnel.

Communication & Collaboration:

- Report security issues and concerns to senior security personnel.
- Collaborate with security professionals to learn best practices and improve security awareness.
- Maintain effective communication with system users regarding security-related matters.

Skills and Qualifications:

- Basic understanding of cybersecurity principles and best practices, including common attack vectors and security frameworks.
- Familiarity with information systems, operating systems, databases, and basic network security concepts.
- Foundational knowledge of risk management and security assessment methodologies.
- Strong analytical and problem-solving skills, with a willingness to learn and develop expertise.
- Effective communication and interpersonal skills, with the ability to convey technical information clearly.
- Strong attention to detail and ability to prioritize tasks in a structured manner.

Certifications:

- CompTIA Security+: A foundational certification demonstrating knowledge of cybersecurity principles.
- Certified Information Systems Security Professional (CISSP) Associate.
- Other entry-level cybersecurity certifications (e.g., GIAC GSEC, Microsoft Security Fundamentals).

Required Experience:

- Minimum of 2 years of experience in cybersecurity, IT security, or a related field. Minimum of two years of experience in IT support, help desk, or related technical role are required (internship, coursework, or part-time IT roles are acceptable for experience.)
- Some experience with security tools such as antivirus software, firewalls, or basic SIEM solutions is a plus.
- Familiarity with incident response and security investigations is beneficial but not required.
- Exposure to risk management and compliance frameworks (e.g., NIST, ISO) is preferred but not required.

CLIN 05 - 07 - Senior Cybersecurity Engineer

The Senior Cybersecurity Engineer is responsible for designing, implementing, and maintaining the organization's cybersecurity infrastructure. This role requires deep technical expertise to ensure robust protection against emerging threats while maintaining compliance with industry standards. The Senior Cybersecurity Engineer will collaborate with IT, security operations, and leadership teams to implement cutting-edge security measures and enhance the organization's security posture.

Key Responsibilities:

Security Architecture and Design:

- Design and implement advanced cybersecurity solutions, including network security, endpoint protection, and cloud security.
- Develop secure architectures for on-premises, cloud, and hybrid environments.
- Evaluate and integrate new security technologies to address evolving threats.

System Implementation and Maintenance:

- Deploy and configure firewalls, Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Endpoint Detection & Response (EDR), Zero Trust Security (ZTS), Security Information & Event Management (SIEM) solutions, and other security tools.
- Perform regular updates, patching, and upgrades to security systems to ensure optimal performance.
- Collaborate with IT teams to secure applications, databases, and servers.

Threat Management and Incident Response:

- Proactively identify, analyze, and remediate vulnerabilities in systems and applications.
- Respond to security incidents, perform root cause analysis, and implement corrective measures.
- Develop and maintain incident response plans, playbooks, and procedures.

Risk Management and Compliance:

- Conduct security risk assessments and recommend strategies to mitigate identified risks.
- Ensure compliance with frameworks such as NIST 800-53, ISO 27001, and SOC 2.
- Participate in audits and provide technical evidence of security controls.

Automation and Optimization:

- Develop scripts and tools to automate repetitive tasks, such as log analysis, vulnerability scanning, and incident triage.
- Optimize security processes to improve response times and reduce manual effort.

Collaboration and Leadership:

- Provide technical leadership and mentorship to junior engineers and security analysts.
- Collaborate with cross-functional teams to align security initiatives with business goals.
- Act as a subject matter expert in technical discussions and projects.

Skills & Qualifications:

Technical Expertise:

- Knowledge of firewalls, Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Endpoint Detection & Response (EDR), Zero Trust Security (ZTS), Data Loss Prevention (DLP), Security Information & Event Management (SIEM) security solutions.
- Expertise in securing cloud platforms and understanding of DevSecOps practices.
- Proficiency in scripting languages such as Python, PowerShell, or Bash for automation.
- Strong understanding of encryption, authentication, and network protocols.

Analytical and Problem-Solving Skills:

- Ability to perform advanced forensic investigations and identify the root cause of security incidents.
- Strong troubleshooting skills and ability to solve complex technical challenges.

Communication and Collaboration:

- Excellent verbal and written communication skills to explain technical concepts to non-technical stakeholders.
- Demonstrated ability to collaborate across teams and drive consensus.

Certifications:

- Certified Information Systems Security Professional (CISSP)
- Certified Information Systems Auditor (CISA)
- GIAC Certified Incident Handler (GCIH)
- Offensive Security Certified Professional (OSCP)
- Certified Cloud Security Professional (CCSP)
- AWS Certified Security Specialty
- Microsoft Azure Security Technologies Certified
- Certified from Zscaler, CrowdStrike, or Splunk vendor programs

Required Experience:

- Minimum of 10 years of experience in cybersecurity roles, including at least 6 years in a hands-on engineering position.
- Proven experience in designing and implementing enterprise-scale security solutions.
- Demonstrated expertise in securing hybrid IT environments and managing complex security projects.
- Experience with security automation and orchestration tools (SOAR).
- Track record of successfully responding to and mitigating high-severity security incidents.

CLIN 05-09 – Jr. Cybersecurity Engineer

Supports the Court's cybersecurity efforts by assisting in the implementation and maintenance of security measures. The Junior Cybersecurity Engineer works under the guidance of senior security staff to help protect digital assets, identify potential threats, and contribute to the overall security posture of the Court.

Key Responsibilities:

Security Assessments & Monitoring:

- Assist in performing vulnerability scans and basic security assessments.

- Monitor security logs for potential threats and escalate issues as needed.
- Support senior engineers in analyzing security incidents and documenting findings.

Implementing & Supporting Security Controls:

- Assist in configuring and managing security tools, such as firewalls and antivirus software.
- Support the deployment of security patches and updates to systems.
- Help maintain security policies and procedures in compliance with industry standards.

Incident Response & Investigation:

- Participate in incident response activities by gathering data and assisting in investigations.
- Document security incidents and remediation efforts.
- Learn forensic analysis techniques to support security investigations.

Learning & Development:

- Stay up to date on emerging cybersecurity threats and best practices.
- Attend training sessions and collaborate with senior security professionals to expand knowledge.
- Support the evaluation of new security technologies and solutions.

Skills & Qualifications:

- Basic understanding of cybersecurity principles and best practices, including common attack vectors and security frameworks.
- Familiarity with networking concepts (TCP/IP, DNS, firewalls) and operating systems (Windows, Linux, macOS).
- Basic knowledge of scripting languages (e.g., Python, PowerShell) is a plus.
- Strong analytical and problem-solving skills with a willingness to learn.
- Effective communication skills to collaborate with technical and non-technical teams.
- Attention to detail and ability to prioritize tasks effectively.

Certifications:

- CompTIA Security+ (or working towards obtaining it).
- Certified Ethical Hacker (CEH)
- Microsoft or AWS security certifications

Required Experience:

- Minimum of two years of experience in cybersecurity, IT security, or a related field. Internship, coursework, or part-time IT roles are acceptable for experience
- Familiarity with security tools such as antivirus software, firewalls, or SIEM solutions is beneficial.
- Exposure to cybersecurity frameworks (e.g., NIST, ISO 27001) is preferred but not required.
- Hands-on experience from coursework, internships, or lab environments is highly valued.

CLIN 05-11 – Cybersecurity Analyst

Responsible for monitoring, analyzing, and responding to security events and potential threats to the Court's information systems. This role provides intermediate-level expertise in cybersecurity operations, risk mitigation, and incident response to ensure the Court's IT environment remains secure and compliant with applicable regulations and standards.

Key Responsibilities:

Security Operations:

- Perform proactive monitoring and analysis of security events using tools such as Security Information & Event Management (SIEM), Zero Trust Security (ZTS), Endpoint Detection & Response (EDR), Intrusion Detection System (IDS), Intrusion Prevention System (IPS) cyber management platforms.
- Investigate and respond to security alerts, ensuring thorough documentation and resolution of incidents.
- Conduct regular vulnerability scans and assist in the remediation of identified risks.

Incident Response:

- Participate in the Court's incident response efforts, including identifying, containing, and remediating threats.
- Assist in the development and maintenance of incident response playbooks.
- Conduct post-incident analysis to improve response times and overall security posture.

Risk Assessment and Mitigation:

- Perform risk assessments on systems, networks, and applications to identify security gaps.
- Recommend and implement controls to mitigate identified vulnerabilities.
- Collaborate with IT teams to ensure secure configurations and compliance with security policies.

Policy and Procedure Compliance:

- Support the development and enforcement of organizational cybersecurity policies and standards.
- Ensure compliance with frameworks such as NIST, ISO 27001, and other relevant standards.
- Conduct periodic security awareness training for employees to promote best practices.

Collaboration and Communication:

- Work closely with senior cybersecurity staff and IT teams to address security challenges.
- Provide clear and concise reports on security incidents, risk assessments, and vulnerabilities to stakeholders.
- Collaborate with external vendors and partners to address third-party security risks.

Knowledge Base Management:

- Maintain and update cybersecurity knowledge base articles for use by Tier 1 staff and other teams.

- Contribute to the Court's continuous improvement by identifying process gaps and recommending enhancements.

Skills & Qualifications:
Technical Expertise:

- Proficiency in employing security tools such as firewalls, Security Information & Event Management (SIEM), Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Zero Trust Security (ZTS), Endpoint Detection & Response (EDR), vulnerability scanning solutions.
- Strong understanding of network protocols, operating systems (Windows, iOS, MacOS, Android), and cloud environments.
- Familiarity with scripting languages (e.g., Python, PowerShell) for automation tasks.

Analytical and Problem-Solving Skills:

- Ability to analyze security logs and events to identify patterns and potential threats.
- Strong troubleshooting skills for resolving intermediate-level security issues.

Communication and Collaboration:

- Effective written and verbal communication skills to convey technical information to non-technical stakeholders.
- Team-oriented mindset with the ability to work collaboratively in a fast-paced environment.

Certifications:

- CompTIA Security+
- AWS Certified Security Specialty
- Microsoft Azure Security Technologies Certified
- Certified from Zscaler, CrowdStrike, or Splunk vendor programs
- Certified Ethical Hacker (CEH)
- GIAC Security Essentials Certification (GSEC)
- Microsoft Certified: Security, Compliance, and Identity Fundamentals

Required Experience:

- Minimum of 3 years of hands-on experience in cybersecurity or related IT roles.
- Practical experience with security monitoring tools and incident response processes.
- Exposure to compliance requirements and risk management frameworks such as NIST or ISO 27001.

CLIN 05-12 Jr. Cybersecurity Analyst

Responsible for assisting in the monitoring, analysis, and response to security events and potential threats to the Court's information systems. This role provides an opportunity to develop expertise in cybersecurity operations, risk mitigation, and incident response while supporting the Court's IT security team in maintaining a secure and compliant IT environment.

The Junior Cybersecurity Analyst will gain hands-on experience with security tools, best practices, and industry standards under the guidance of senior team members.

Key Responsibilities:

Security Operations:

- Assist in monitoring and analyzing security events using tools such as Security Information & Event Management (SIEM), Endpoint Detection & Response (EDR), and Intrusion Detection/Prevention Systems (IDS/IPS).
- Support the investigation of security alerts and document findings for review by senior analysts.
- Help conduct vulnerability scans and track remediation efforts to ensure security risks are addressed.
- Learn and apply security best practices for IT systems and applications.

Incident Response:

- Participate in incident response activities under the supervision of senior cybersecurity staff.
- Assist in documenting security incidents, remediation steps, and lessons learned.
- Help maintain and update incident response playbooks to improve response processes.

Risk Assessment and Mitigation:

- Support risk assessments on systems, networks, and applications to help identify potential vulnerabilities.
- Work with IT teams to apply basic security controls and ensure compliance with security policies.
- Learn how to review security configurations and settings to help strengthen system defenses.

Policy and Compliance:

- Assist in maintaining security policies, procedures, and best practices.
- Help track compliance with industry frameworks such as NIST and ISO 27001.
- Support security awareness initiatives by helping develop training materials and resources.

Collaboration and Learning:

- Work closely with senior cybersecurity staff and IT teams to gain hands-on experience in security operations.
- Participate in training programs and mentorship opportunities to build cybersecurity expertise.
- Assist in preparing security reports and summaries for internal stakeholders.
- Engage with external vendors and security partners to support third-party security assessments.

Skills & Qualifications:

- **Technical Skills:**

- Basic understanding of security tools such as SIEM, IDS/IPS, EDR, firewalls, and vulnerability scanners.
- Foundational knowledge of network protocols, operating systems (Windows, macOS, Linux, iOS, Android), and cloud environments.
- Interest in learning scripting languages (e.g., Python, PowerShell) for basic automation tasks.
- Familiarity with cybersecurity principles, including access controls, encryption, and endpoint security.

- **Analytical and Problem-Solving Skills:**
- Ability to analyze basic security logs and recognize potential security issues.
- Strong attention to detail when documenting security events and findings.
- Willingness to learn troubleshooting techniques for common security challenges.

- **Communication and Collaboration:**
- Effective verbal and written communication skills to document security incidents and findings.
- Ability to work collaboratively in a team environment and follow guidance from senior analysts.
- Strong willingness to learn, ask questions, and take initiative in a cybersecurity role.

Certifications:

- CompTIA Security+ (or willingness to obtain within the first year)
- Microsoft Certified: Security, Compliance, and Identity Fundamentals
- AWS Certified Cloud Practitioner
- GIAC Security Essentials Certification (GSEC)
- Certified Ethical Hacker (CEH)

Required Experience:

- Minimum of 2 years of experience in cybersecurity, IT support, or a related field. Internship, coursework, or part-time IT roles are acceptable for experience.
- Familiarity with basic cybersecurity concepts through coursework, internships, or personal projects.
- Exposure to security tools and technologies in a lab environment or academic setting is a plus.

H.4.5 Optional Project Support CLINs – These are not Staff Augmentation CLINs and can therefore not be called LCATs. Project Support CLINs will also be priced as FFP.

CLIN 06-01 Project Management

This CLIN, if executed, would provide the Court with comprehensive project management services for one or more specified projects, ensuring effective oversight and delivery of projects by managing cost, schedule, performance, and risk. The contractor will provide skilled project managers and support staff to coordinate activities, monitor progress, and deliver outcomes aligned with organizational objectives. These services are essential for maintaining operational efficiency, meeting project milestones, and minimizing risks.

Key responsibilities include developing and maintaining project schedules, tracking budgets to ensure cost containment, and identifying and mitigating risks throughout the project lifecycle. The contractor will implement performance monitoring systems and provide regular reports to stakeholders, detailing project status, variances, and corrective actions. By employing industry-standard project management methodologies, the contractor will ensure all deliverables meet quality standards and timelines.

Additionally, the contractor will establish effective communication channels to engage stakeholders, facilitate decision-making, and resolve issues as they arise. Services also include conducting post-project evaluations to capture lessons learned and improve future project outcomes. This CLIN ensures that projects are managed with precision and accountability, enabling clients to achieve strategic goals while minimizing disruptions and resource inefficiencies.

CLIN 06-02 Physical Access Control System Support

This CLIN provides targeted support for discrete projects related to the Court's Physical Access Control System (PACS) at both the Washington, DC Courthouse and Field Courtroom facilities. The contractor will deliver services focused on minor maintenance (e.g., troubleshooting and replacing control panels) and minor installations (e.g., installation of card readers or intercoms during renovations), ensuring secure and efficient access management for authorized personnel across all court locations.

Key responsibilities include performing preventative maintenance and addressing issues as they arise, such as resolving badge or credential malfunctions and troubleshooting system outages. The contractor will also support discrete installation projects, such as the addition of new card readers, biometric scanners, or intercom systems to accommodate renovations or modifications to existing facilities. These activities will be performed with minimal disruption to ongoing operations.

Additionally, the contractor will document system updates and provide clear instructions to court personnel for the proper operation of new or modified components.
o n-call support will be available to respond to urgent needs, ensuring that PACS components remain operational and effective. These services are critical for maintaining the functionality and security of access control systems in support of the Court's mission.

CLIN 06-03 Courtroom System Support

Description: This CLIN covers all services related to the design, installation, and maintenance of the IT infrastructure within the Court's Field Courtrooms.

System Engineering and Architecture:

- Design, document, and implement network solutions for Field Courtrooms, including:
  - Network topology and architecture.
  - Selection and sizing of network devices (switches, routers, wireless access points).
  - Network security protocols and configurations (firewalls, intrusion detection/prevention systems - where applicable).
  - Network performance monitoring and troubleshooting tools.
  - Integration with existing or planned agency-wide network infrastructure.
- Develop and maintain network documentation, including diagrams, configurations, and procedures.

Installation:

- Install, configure, and test all network equipment within Field Courtrooms according to design specifications and best practices.
- Perform cable installations and terminations adhering to industry standards.
- Commission and integrate network devices into the overall network environment.

Maintenance:

- Provide ongoing maintenance and support for all installed network equipment, including:
  - Proactive monitoring of network performance and health.
  - Troubleshooting and resolution of network issues.
  - Scheduled and on-demand maintenance activities (e.g., firmware upgrades, software patches).
  - Emergency response and repair services for network outages.
- Maintain network inventory and documentation.

Exclusions: This CLIN does not include:

- Support for end-user devices (laptops, desktops, tablets, phones).
- Support for software applications (other than network-related software).
- Audio-visual equipment support (projectors, microphones, speakers).
- User training or support.
- Procurement of any hardware or software (except for minor consumable items as approved).

Deliverables:

- Network design documentation.
- Installation reports.
- Network maintenance reports.
- Network diagrams and documentation.

CLIN 06-04 Financial System Support

This CLIN encompasses all services related to the ongoing support, maintenance, and modernization of the Court's Financial System. This includes comprehensive support for existing legacy systems, ensuring their continued operation and stability. Furthermore, this CLIN covers the design, implementation, and migration support for modernizing the Court's financial operations.

Legacy System Support:

- Provide ongoing maintenance and support for existing legacy financial systems, including:
    - Troubleshooting and resolution of system issues and errors.
    - Application of software patches and updates.
    - Data backups and recovery procedures.
    - User support and assistance.
    - Proactive system monitoring and performance tuning.

Modernization Support:

- Design, develop, and implement a modernized financial system architecture, including:
    - System engineering and architecture design.
    - Software development and integration.
    - Data migration planning and execution.
    - User acceptance testing and training.
    - Implementation and deployment support.

Conduct thorough analysis of current business processes and identify areas for improvement.
Develop and implement a phased approach to system modernization.
Ensure compatibility with existing court systems and applications.

CLIN 06-05 Audio/Video System Support

This CLIN provides targeted support for discrete projects related to the Court’s Audio/Video (A/V) systems in the courtrooms, conference rooms, and meeting spaces in the DC Courthouse and Field Courtrooms. If executed, the contractor may be expected to provide end-to-end solutions, including the design, implementation, troubleshooting, and maintenance of advanced A/V systems. Services will ensure seamless integration and standardization of technologies to facilitate effective communication, presentations, and remote collaboration while adhering to high-quality standards and operational reliability.

Key tasks include conducting needs assessments to determine optimal A/V system configurations for specific room types and use cases. The contractor will design systems that

incorporate sound reinforcement, video displays, microphones, cameras, and control systems, ensuring compatibility with existing infrastructure. Troubleshooting services will address system failures or performance issues, minimizing downtime and ensuring user satisfaction. Implementation activities will include hardware installation, software configuration, and testing to confirm the systems meet functional and technical specifications.

Maintenance support will ensure continued system functionality, including routine inspections, firmware updates, and user training. The contractor will also provide on-demand technical assistance to resolve emergent issues if not resolved by the help desk, ensuring that courtrooms, conference rooms, and meeting rooms remain fully operational. These services are critical to supporting the mission requirements of clients and ensuring seamless operations in high-stakes environments.

CLIN 06-06 Cloud Services Support

This CLIN cover the provision of professional services to support large-scale cloud services projects, such as cloud migrations, cybersecurity upgrades, audits, and architecture refactoring to eliminate legacy services. The contractor will ensure cloud environments remain scalable, secure, and aligned with the operational needs of the Court.

Key responsibilities include conducting software-based changes to cloud services employing a Court provided DevOps toolchain. The contractor will ensure use of best practices such as advanced cybersecurity measures, such as zero trust architectures, identity and access management (IAM) upgrades, and vulnerability remediation to enhance the security posture of cloud environments.

In addition, the contractor will perform detailed audits of existing cloud architectures to identify inefficiencies, compliance gaps, and areas for optimization. Refactoring efforts will focus on replacing outdated or unsupported services with cost-effective, cloud-native solutions that improve performance and scalability while reducing technical debt.

Documentation, source code, and knowledge transfer are essential components of this CLIN, ensuring stakeholders understand system changes and can maintain operations post-implementation. These discrete projects are critical to enhancing the Court’s cloud infrastructure, ensuring long-term operational success and resilience.

CLIN 06-07 Software-As-A-Service Support

This CLIN covers the provision of professional services to support discrete projects that modernize the Court's judicial or non-judicial operations through the implementation and utilization of Software-as-a-Service (SaaS) solutions. This includes project management, system analysis, design, implementation, integration, and ongoing support for selected SaaS applications.

Scope of Work:

- Project Management:
    - Define project scope, objectives, timelines, and budgets.
    - Develop and manage project plans, including resource allocation, risk mitigation, and change management.
    - Conduct regular project reviews and report on progress and status.

- SaaS Solution Evaluation and Selection:

    - Assist the Court in evaluating and selecting appropriate SaaS solutions based on functional requirements, budget constraints, and vendor capabilities.
    - Conduct vendor assessments and negotiate contracts.
- SaaS Implementation and Integration:
    - Configure and customize SaaS applications according to Court requirements.
    - Integrate SaaS solutions with existing court systems and applications.
    - Develop and implement data migration plans.
    - Conduct user training and provide ongoing support.
- Ongoing Support:
    - Provide ongoing support for implemented SaaS solutions, including:
        - Troubleshooting and resolution of system issues.
        - Application of software updates and patches.
        - System monitoring and performance tuning.
        - User support and assistance.
    - Monitor industry trends and recommend new SaaS solutions as needed.

CLIN 06-08 Library Information System Support

This CLIN covers the provision of professional services to support the modernization of the Court's library information systems. This includes systems analysis and design, implementation, integration, and transition for projects related to the enhancement, replacement, or integration of library technologies.

- Systems Analysis and Design:

    - Conduct needs assessments and feasibility studies for library technology projects.
    - Develop system requirements and specifications.
    - Design and document system architectures and workflows.

- Implementation and Integration:

    - Oversee the implementation and integration of new library technologies, including:
        - Library Management Systems (LMS)

- Digital Library platforms
- Electronic Resource Management Systems (ERMS)
- Discovery services
- Learning Management Systems (LMS)
- Library website and online services

Conduct user training and provide ongoing support.

CLIN 06-09 Hardware and associate Software Refresh Support

This CLIN covers the provision of professional services to support the planning, procurement, deployment, and transition of hardware as part of a refresh cycle. This includes a wide range of IT equipment such as printers, scanners, laptops, smartphones, switches, routers, servers, and any associated software (e.g., firmware, drivers).

- Hardware Planning and Procurement:
    - Assist in the planning and budgeting for a hardware refresh cycle including researching evolving standards, identification of suitable replacements brands and models, and identify any major changes or risks required to perform the refresh.
    - Analyze the refresh options identifying tradeoffs amongst performance, budget, and user requirements.

- Hardware Deployment and Configuration:
    - Manage the deployment and installation of new hardware, including:
        - On-site installation and configuration.
        - Software installation and driver updates.
        - Network connectivity and configuration.
        - Data migration and user data transfer.
    - Provide user training and support on new hardware and software.

- Transition:
    - Provide ongoing, short-term support for the deployed system (not to exceed three months) and work to transition hardware operations and maintenance to the Court's staff, including:
        - Troubleshooting and resolution of hardware and software issues.
        - Proactive maintenance and preventative measures.
        - Hardware repairs and replacements.
        - Inventory management and tracking.
        - Knowledge transition including system training, provisioning technical data as well as providing standard procedures.

- Develop and transition a plan for the hardware's lifecycle management to inform planning for the next refresh.

CLIN 06-10 System Engineering and Architecture Support

This CLIN covers the provision of professional services for system engineering and architecture support related to the planning and design of large-scale projects. These services focus on advanced design and planning activities, excluding the actual implementation of the project itself.

Scope of Work:

- System Requirements Definition:
  - Elicit, analyze, and document system requirements from stakeholders.
  - Develop and maintain system requirements specifications.
  - Conduct feasibility studies and gap analyses.
- System Architecture Design:
  - Develop and document system architectures, including:
    - High-level and detailed design diagrams.
    - Component and interface definitions.
    - Data flow diagrams.
    - Technology selection and justification.
  - Conduct trade-off analyses and select optimal solutions.
- Technical Documentation:
  - Develop and maintain comprehensive technical documentation, including:
    - System requirements specifications.
    - System architecture documents.
    - Design documents.
    - Interface control documents.
- Technical Support:
  - Provide technical guidance and support to project teams during the planning and design phases.
  - Participate in design reviews and technical meetings.
  - Address technical questions and resolve technical issues.

CLIN 06-11 Cybersecurity Incident Response

This CLIN covers the provision of professional cybersecurity incident response services to effectively manage and mitigate the impact of **suspected** cybersecurity incidents. This includes incident validation, incident resolution, residual risk assessment, and restoring normal court operations following an incident.

- Incident Validation and Assessment:
  - Rapidly assess and validate suspected cybersecurity incidents, including:
    - Analyzing security logs, alerts, and other relevant data.
    - Conducting initial threat intelligence gathering.

        - Determining the scope and potential impact of the incident.
- Incident Resolution:
    - Implement containment and isolation measures to limit the spread of the incident.
    - Conduct in-depth incident analysis to determine the root cause and scope.
    - Coordinate with relevant stakeholders (e.g., IT, legal, human resources, law enforcement).
    - Implement remediation actions to address identified vulnerabilities and weaknesses.
- Residual Risk Assessment:
    - Conduct a thorough assessment of residual risks following an incident.
    - Develop and implement measures to mitigate identified residual risks.
    - Document and communicate residual risks to relevant stakeholders.
- Restoration of Normal Operations:
    - Assist in the restoration of normal court operations following an incident.
    - Oversee the recovery and restoration of critical systems and data.
    - Conduct post-incident activities, including system hardening and security enhancements.

CLIN 06-12 Vulnerability Assessment & Penetration Testing

This CLIN covers the provision of professional penetration testing services to identify and assess vulnerabilities in specified systems or applications. The penetration testing will simulate real-world cyberattacks to uncover exploitable weaknesses in the Court's target environment(s), system(s), or application(s).

- Penetration Testing Execution:
    - Conduct comprehensive penetration testing activities, including:
        - Network penetration testing (e.g., vulnerability scanning, port scanning, exploitation attempts).
        - Application penetration testing (e.g., web application testing, mobile application testing, API testing).
        - Social engineering testing (e.g., phishing simulations, pretexting).
        - Wireless network testing.
        - Cloud environment testing.
    - Utilize a variety of tools and techniques to identify vulnerabilities, such as:
        - Automated scanning tools.
        - Manual testing techniques.
        - Exploitation tools.
- Vulnerability Assessment and Reporting:
    - Document and categorize identified vulnerabilities according to severity (e.g., critical, high, medium, low).
    - Provide detailed reports on all identified vulnerabilities, including:

        - Vulnerability descriptions.
        - Proof-of-concept exploits (where applicable).
        - Remediation recommendations.
        - Risk assessments.
    - Work with the Court staff to develop a POA&M for remediating the greatest risks found.

- Project Management:

    - Coordinate testing activities with the Court to minimize disruption to normal operations.
    - Maintain clear and concise communication throughout the engagement.
    - Deliver timely reports and updates on testing progress.

CLIN 06-13 Cybersecurity Training for End Users

This CLIN covers the provision of professional cybersecurity awareness training services to all Court personnel. Training will focus on enhancing cybersecurity awareness and best practices to reduce the risk of cyberattacks.

Scope of Work:

- Cybersecurity Awareness Training:

    - Develop and deliver interactive cybersecurity awareness training programs, including:
        - In-person training sessions.
        - Online training modules.
        - Simulated phishing exercises.
        - Awareness campaigns and communications.
    - Cover a wide range of cybersecurity topics, including:
        - Phishing and social engineering threats.
        - Malware and ransomware attacks.
        - Data security and privacy best practices.
        - Secure password management.
        - Safe internet browsing and email practices.
        - Mobile device security.
        - Social media security.
        - Insider threats.

- Phishing Email Tests:

    - Conduct simulated phishing email tests to assess user awareness and response rates.
    - Analyze test results and provide feedback to Court leadership.

- Track and report on phishing test results and overall user awareness levels.

- Cybersecurity Awareness Campaigns:

  - Develop and implement targeted cybersecurity awareness campaigns to reinforce key messages and best practices.
  - Utilize various communication channels, such as email, intranet, posters, and newsletters.
  - Provide timely updates on emerging cyber threats and best practices.

CLIN 06-14 Cybersecurity Project support

This CLIN covers the provision of professional services for the design, implementation, and transition of large-scale cybersecurity modernization projects. This includes a comprehensive approach to enhancing the Court's overall cybersecurity posture through the implementation of advanced security technologies and best practices.

- Cybersecurity Architecture and Design:
  - Conduct a comprehensive cybersecurity risk assessment and gap analysis.
  - Design and document a target cybersecurity architecture, including:
    - Recommendations and selection and integration of security technologies (e.g., next-generation firewalls, intrusion detection systems, endpoint security solutions, cloud security solutions).
    - Implementation of security controls (e.g., multi-factor authentication, access control, data loss prevention).
    - Development of security policies and procedures.
  - Develop a detailed project plan for the implementation of the cybersecurity modernization project.
- Implementation and Integration:
  - Procure, deploy, and configure new cybersecurity technologies.
  - Integrate new security solutions with existing IT infrastructure.
  - Conduct thorough testing and validation of implemented security controls.
  - Provide user training and support on new security technologies and procedures.
- Transition and Ongoing Support:
  - Develop and implement a transition plan for the new cybersecurity environment.
  - Provide ongoing support and maintenance for implemented security solutions.
  - Monitor security alerts and incidents.
  - Conduct regular security assessments and penetration testing.
  - Continuously evaluate and improve the Court's cybersecurity posture.

CLIN 06-15 Audit Preparation Support

This CLIN covers the provision of professional services to support the preparation for and response to audits. This includes internal assessments of controls, identification and documentation of control weaknesses, development of recommendations to resolve identified issues, development and implementation of Plans of Action and Milestones (POA&Ms), and ongoing monitoring of progress on the POA&M.

- Internal Controls Assessment:
    - Conduct internal assessments of controls relevant to the audit scope, including:
        - Risk assessments.
        - Control walkthroughs and testing.
        - Documentation of control procedures.
        - Identification and documentation of control weaknesses.
- Issue Resolution and Recommendations:
    - Develop and document recommendations to address identified control weaknesses.
    - Conduct root cause analysis to identify the underlying causes of control failures.
    - Develop and implement corrective action plans.
- POA&M Development and Monitoring:
    - Develop and implement a comprehensive POA&M to track progress on the resolution of audit findings.
    - Monitor progress on the implementation of corrective actions.
    - Update and maintain the POA&M on a regular basis.
    - Report on the status of corrective actions to management.
- Audit Support:
    - Provide support to internal and external auditors during the audit process.
    - Respond to audit inquiries and provide requested information.
    - Assist in the preparation of audit responses.

CLIN 06-16 Audit Support

This CLIN covers the provision of professional services to support the conduct of IT audits. This includes assisting audit teams in gathering IT audit evidence, assessing IT controls, and addressing IT audit findings.

Scope of Work:

- IT Control Assessments:

    - Assist audit teams in assessing the effectiveness of IT controls, including:
        - Access controls.
        - Change management controls.
        - Data security controls.
        - Network security controls.

        - Disaster recovery and business continuity controls.
    - Provide documentation and evidence of IT controls.

- IT Audit Evidence Gathering:

    - Assist audit teams in gathering IT audit evidence, such as:
        - System logs.
        - Network traffic data.
        - Security incident reports.
        - User access logs.
        - Vulnerability scan reports.
    - Prepare and analyze data for audit purposes.

- IT Audit Findings Remediation:

    - Assist in the remediation of IT audit findings, including:
        - Developing and implementing corrective action plans.
        - Implementing security enhancements.
        - Improving IT control processes.
        - Providing technical expertise to address audit observations.

CLIN 06-17 Software Development Project Support

This CLIN covers the provision of all professional services required for the successful completion of a major software development project beyond the Court staff and staff augmentees capacity. This includes all phases of the software development lifecycle traversed with agile methodologies, from requirement gathering and design to development, testing, implementation, and transition. The project would employ the Court provided DevOps Toolchain and transition the operations and maintenance to Court staff and staff augments.

- Software Development Lifecycle:

    - Requirements gathering and analysis.
    - System design and architecture.
    - Software development and coding.
    - Software testing (unit testing, integration testing, system testing, user acceptance testing).
    - Deployment and implementation.
    - User training and support.
    - Ongoing maintenance and support.

- Project Management:

    - Project planning and scheduling.
    - Risk management and issue resolution.
    - Resource allocation and management.

- Quality assurance and control.
- Progress monitoring and reporting.
- Change management.

- Deliverables:

  - Software deliverables (source code, executable files, documentation).
  - Project plans and schedules.
  - Test plans and reports.
  - User manuals and training materials.
  - Project status reports.

CLIN 06-18 Strategic Initiative Project Support

This CLIN covers the provision of all professional services required for the successful implementation of a major IT project. This includes project management, systems analysis and design, development, testing, implementation, and transition of the operations and maintenance.

- Project Management:

  - Define project scope, objectives, timelines, and budgets.
  - Develop and manage project plans, including resource allocation, risk mitigation, and change management.
  - Conduct regular project reviews and report on progress and status.

- Systems Analysis and Design:

  - Conduct needs assessments and feasibility studies.
  - Develop system requirements and specifications.
  - Design and document system architectures and workflows.

- Implementation and Integration:

  - Oversee the implementation and integration of new IT systems and technologies.
  - Conduct user training and provide temporary ongoing support during transition.
  - Develop and implement data migration plans.
  - Conduct system testing and user acceptance testing.

- Transition:

  - Provide ongoing support for implemented IT systems while transitioning the operations and maintenance of the solution to Court staff and staff augmentees, including:
    - Troubleshooting and resolution of system issues.

- Application of software updates and patches.
- System monitoring and performance tuning.
- User support and assistance.

CLIN 06-19 Human Resources System Support

This CLIN covers the provision of professional services to the ongoing support, maintenance, and modernization of the Court's Human Resource (HR) Systems. This includes comprehensive support for existing legacy HR systems, ensuring their continued operation and stability. Furthermore, this CLIN covers the design, implementation, and migration support for modernizing the Court's HR operations.

Legacy HR System Support:

- Provide ongoing maintenance and support for existing legacy HR systems, including:
  - Troubleshooting and resolution of system issues and errors.
  - Application of software patches and updates.
  - Data backups and recovery procedures.
  - User support and assistance.
  - Proactive system monitoring and performance tuning.
  - Ensure compliance with all applicable laws and regulations related to HR data management and privacy.

HR System Modernization Support:

- Design, develop, and implement a modernized HR system architecture, including:
  - System engineering and architecture design.
  - Software development and integration.
  - Data migration planning and execution.
  - User acceptance testing and training.
  - Implementation and deployment support.
- Conduct thorough analysis of current HR processes and identify areas for improvement, such as:
  - Recruitment and onboarding.
  - Performance management.
  - Training and development.
  - Compensation and benefits administration.
  - Employee relations.
- Develop and implement a phased approach to system modernization.
- Ensure compatibility with existing court systems and applications.