

JASINT Innovative Solutions

Commercial Price List — Cybersecurity Professional Services

1. Company Overview

JASINT Innovative Solutions (JASINT) provides professional consulting and advisory services to Federal, State, and Local government agencies and Commercial Clients. This Commercial Price List reflects our standard published rates for the labor categories listed below. Rates are fully burdened and inclusive of overhead, G&A, and profit.

2. Labor Categories & Rates

The following rates represent our standard commercial pricing. All rates are quoted in U.S. Dollars. Daily rates are based on an 8-hour workday.

Labor Category	Hourly Rate
Senior Penetration Tester	276.57
Senior Cyber Hunter	285.64
Cyber Data Architect	262.97
Cyber Security Engineer	249.37
Cyber Network Engineer	240.30
Cyber Enterprise Architect	276.57
Cyber Subject Matter Expert	358.19
Cyber Senior Program Manager	358.19

3. Terms & Conditions

- Payment Terms: Net 30 days from date of invoice unless otherwise negotiated.
- Travel & ODCs: Travel expenses and other direct costs (ODCs) are billed at cost, not to exceed amounts agreed upon in the applicable task order or contract.
- Overtime: Work performed in excess of 40 hours per week or on federal holidays will be billed at 1.5x the applicable hourly rate, subject to prior client approval.
- Rate Escalation: Rates are subject to annual adjustment, typically not to exceed 3% per year, effective on the anniversary of the contract.

- **Minimum Engagement:** A minimum engagement of 40 hours applies to all labor categories unless otherwise agreed in writing.
- **Cancellation:** Engagements may be terminated with 30 days' written notice. Work performed through the effective termination date will be invoiced at the applicable rates.

4. Labor Category Descriptions

Detailed descriptions of each labor category, including functional responsibilities and minimum qualifications, are provided below.

4.1. Senior Penetration Tester

May respond to crisis or urgent situations to mitigate immediate and potential threats. Approaches may include the use of information and threat intelligence specifically focused on a proximate incident to identify undiscovered attacks. Investigates and analyzes all relevant response activities. Identifies and assesses the capabilities and activities of cyber criminals or foreign intelligence entities; design and administer procedures in the organization that sustains the security of the organization's data and access to its technology and communications systems. Duties may include Lead Cyber Hunt team, provides oversight and be responsible for event investigation and tracking activities. Identifies, deters, monitors, and investigates computer and network intrusions. Provide computer forensic support to high technology investigations in the form of evidence seizure, computer forensic analysis, and data recovery

4.2. Senior Cyber Hunter

May support in part or in whole technical vulnerability assessments of applications and infrastructure, vulnerability research, and generation of assessment reports. Duties include: May devise and / or select appropriate technical tests, network or vulnerability scan tools, and/or pen testing tools based on review of requirements and purpose; lists all steps involved for executing selected test(s) and coaches others in the use of advanced research, development, or scan tools and the analysis of comparative findings between proposed and current technologies Coordinates or leads teams to conducts ethical tests, network scans, and/or vulnerability scans that support the evaluation of information safeguard effectiveness Conduct reconnaissance, target assessment, target selection, and vulnerability research Creates custom tools and exploits to penetrate various levels of controls including network, operating system, and physical Using COTS or custom tools, conduct or leads teams to conduct vulnerability assessments, analyzes results, identifies exploitable vulnerabilities, and verifies vulnerabilities through manual assessment.

4.3. Cyber Data Architect

The Cyber Data Architect may define, design, or develop relational and/or multi-dimensional databases for warehousing of data. The Cyber Data Architect reviews current data structures and recommends optimizations and reconfigurations as warranted.

4.4. Cyber Security Engineer

Participate in special projects or investigations into specific technology or solution issues; research and pilot demonstration of new technologies. Serve as a point of contact for engineering efforts while maintaining compliance with the customers' policies and guidelines. Duties may include Configure and maintain policies. Maintain documentation for exceptions to standards. Provides timely and adequate response to threats/alerts

4.5. Cyber Network Engineer

Provides engineering services and support related to security/cybersecurity investigations, recovery, and/or response. The scope of responsibility relates to one or more of the following IT areas: information/data, computer hardware or software, networks, mobile computing, cloud, and/or applications. Specialized tasks may include but are not limited to ethical hacking, penetration testing or risk and vulnerability assessment (RVA), whether related to potential or actual threats, attacks, incidents, forensics, intrusions, and/or responses/remediations.

4.6. Cyber Enterprise Architect

The Cyber Enterprise Architect works with stakeholders, both leadership and subject matter experts, to build a holistic view of the organization's strategy, processes, information, and information technology assets to ensure that the business and IT are in alignment and protected from cyber threats. The Cyber Enterprise Architect links the business mission, strategy, and processes of an organization to its IT strategy - including security, and documents this using multiple architectural models or views that show how the current and future needs of an organization will be met in an efficient, sustainable, agile, secure, and adaptable manner.

4.7. Cyber Subject Matter Expert

The Cybersecurity SME will represent the company and provide technical leadership to project teams. The position will advise corporate officers on business strategy staying abreast of current technologies. The SME will also provide project management, pre-sales briefings, and proposal writing support. Provide documentation to Customer which describes all identified system risks, planned test procedures taken, and test results. Provide enhancement capabilities and SOPs to assessment operations for execution and implementation. Maintain accountability to endure integrity and confidentiality of the process. Provide analysis of vulnerabilities. Review and make recommendations on program-level documentation (e.g., requirements specification, system architecture, design documents, test plans, security plans, etc.). Develop and document security evaluation test plan and procedures. Assist in researching, evaluating, and developing relevant Information Security policies and guidance

4.8. Cyber Senior Program Manager

The Senior Cyber Program Manager has overall accountability for Cyber programs. Senior Program Managers may be responsible for product delivery and financial management of client engagements. A Senior Cyber Program Manager performs independent quality assurance reviews of program performance and deliverables to ensure that contractual obligations are being met.

5. Contact Information

JASINT Innovative Solutions

9730 Patuxent Woods Drive, Suite 500

Columbia, MD 21046

Phone: (410) 969-5573

Email: contracts@jasint.com

Website: www.jasint.com