MINISTERSTWO SPRAWIEDLIWOŚCI
www.ms.gov.pl

Warszawa, dnia 09 kwietnia 2021 r.

BIURO CYBERBEZPIECZEŃSTWA

BC-II.252.1.2021

Zaproszenie do złożenia oferty na dostawę przeprowadzenie szkolenia i egzaminu CompTIA Security+

Zamawiający – Ministerstwo Sprawiedliwości zaprasza do złożenia oferty na przeprowadzenie szkolenia i egzaminu CompTIA Security+.

W ramach rozeznania rynku oraz w celu oszacowania wartości zamówienia, w tym kosztów realizacji zamówienia, Ministerstwo Sprawiedliwości zaprasza Państwa do przesłania wstępnej kalkulacji ceny. W przedstawionej kalkulacji cenowej należy podać ceny netto i brutto w złotych, zgodnie z formularzem cenowym stanowiący załącznik nr 3 do niniejszego zapytania.

Wymagania i warunki realizacji dotyczące przedmiotu zamówienia zostały określone w Opisie przedmiotu zamówienia oraz Istotnych postanowieniach umowy – Załączniki nr 1 i nr 2 do niniejszego zaproszenia.

Ofertę cenową należy przedstawić zgodnie ze wzorem stanowiącym Załącznik nr 3 do Zaproszenia.

Ofertę należy złożyć w terminie do dnia 28 kwietnia 2021 r., do godz. 12:00, w formie elektronicznej format PDF, na adres Kamil.Krawiec@ms.gov.pl oraz Mariusz.Klimecki@ms.gov.pl

Zamawiający informuje, że przedmiotowe zaproszenie nie stanowi ofert w rozumieniu art. 66 KC, ani też nie jest ogłoszeniem o zamówieniu w rozumieniu ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych (Dz. U. z 2019, poz. 2019).

Załączniki:

1. Opis Przedmiotu Zamówienia;
2. Wzór umowy;
3. Formularz cenowy.

Załącznik nr 1
do zamówienia nr BC-II.252.1.2021

Opis przedmiotu zamówienia I.

Przedmiot zamówienia:

Przeprowadzenie szkoleń z zakresu egzaminu CompTIA Security+ (SY0-601) oraz organizacja egzaminu certyfikacyjnego.

II. Termin wykonania zamówienia:

Od dnia zawarcia umowy do dnia 20 grudnia 2021 roku.

III. Zakres i wymagania szczegółowe CompTIA Security+ (SY0-601):

1. Szkolenia i egzamin zostaną przeprowadzone do 20 grudnia 2021 roku.
2. W szkoleniu i egzaminach uczestniczyć będzie pięciu pracowników Zamawiającego.
3. Każdy uczestnik otrzyma dokument poświadczający ukończenie szkolenia.
4. Szkolenia i egzaminy muszą zostać przeprowadzone w języku polskim lub angielskim.
5. Wykonawca zobowiązuje się do zaproponowania co najmniej jednego terminu szkolenia do wyboru przez Zamawiającego.

Załącznik nr 2
do zamówienia nr BC-II.252.1.2021

Wzór umowy

Umowa nr……

Umowa zawarta w dniu …….. 2021 r. w Warszawie pomiędzy: **Skarbem Państwa - Ministerstwem Sprawiedliwości** w Warszawie przy Al. Ujazdowskie 11, 00-567 Warszawa, NIP: 52616-73-166, REGON: 000319150, zwanym w dalszej części Umowy **„Zamawiającym”**, reprezentowanym przez:

…….

a

……,

zwanym w dalszej części Umowy **„Wykonawcą”**,

o następującej treści :

§ 1

Przedmiot Umowy

1. W ramach Umowy, Wykonawca zobowiązuje się na rzecz Zamawiającego do:
   1) przeprowadzenia szkolenia przygotowującego do egzaminu CompTIA Security+ SY0-601 dla pięciu osób,
   2) przeprowadzenia egzaminu certyfikacyjnego CompTIA Security+ SY0-601 dla pięciu osób.
2. Szczegółowy Opis Przedmiotu Zamówienia zawiera Załącznik nr 1 do umowy.
3. Miejsce przeprowadzenia szkoleń pozostaje do wyboru Wykonawcy, z zastrzeżeniem, że musi się znajdować na terenie Warszawy lub być przeprowadzone w formie zdalnej.

§ 2 Termin realizacji Umowy

1. W terminie do 5 dni roboczych od zawarcia Umowy, Wykonawca jest zobowiązany do wskazania co najmniej jednego terminu przeprowadzenia szkolenia i egzaminu do wyboru Zamawiającego.
2. Wykonawca zobowiązuje się do przeprowadzenia szkolenia w terminie nie później niż do 20 grudnia 2021 roku.
3. Wykonawca zobowiązuje się do przeprowadzenia egzaminu nie wcześniej niż 2 miesiące i nie później niż 5 miesięcy licząc od dnia zakończenia szkolenia.
4. Przeprowadzenie szkolenia i egzaminu zostanie potwierdzone odpowiednim protokołem, podpisanym przez Zamawiającego, w terminie do 7 dni od dnia zakończenia szkolenia lub egzaminu, zgodnie ze wzorami stanowiącymi Załącznik nr 2 i nr 3 do Umowy.

§ 3 Wynagrodzenie oraz warunki płatności

1. Za wykonanie całego przedmiotu umowy, Zamawiający zapłaci Wykonawcy wynagrodzenie całkowite w wysokości …… zł brutto (słownie: ……), w tym:
   1) za przeprowadzenie szkolenia dla 5 osób w wysokości: …….. zł brutto (słownie: ……..), 2) za przeprowadzenie egzaminu dla 5 osób w wysokości: …… zł brutto (słownie: ……..).
2. Wynagrodzenie całkowite określone w ust. 1 zawiera wszelkie koszty związane z realizacją Umowy, w tym opłaty, podatki i należności wynikające z obowiązujących przepisów prawa, jak również koszt przeprowadzenia szkolenia i egzaminu, zgodnie z wyszczególnionymi w Opisie Przedmiotu Zamówienia wytycznymi.
3. Wynagrodzenie płatne będzie po przeprowadzeniu szkolenia w wysokości określonej w ust. 1 pkt 1 oraz po przeprowadzeniu egzaminu w wysokości określonej w ust. 1 pkt 2.
4. Podstawą do wystawienia faktury będzie podpisany bez zastrzeżeń przez Zamawiającego odpowiedni protokół odbioru.
5. Płatność dokonana będzie na podstawie faktury wystawionej na Ministerstwo Sprawiedliwości, Al. Ujazdowskie 11, 00-950 Warszawa, NIP 5261673166, przelewem bankowym z rachunku Zamawiającego na rachunek Wykonawcy wskazany na fakturze, w terminie 21 dni od otrzymania prawidłowo wystawionej faktury.
6. Za dzień zapłaty uważa się dzień obciążenia rachunku bankowego Zamawiającego.

§ 4 Osoby do kontaktu

1. Ze strony Zamawiającego, osobami odpowiedzialnymi za realizację Umowy oraz upoważnionymi do kontaktu i do podpisania protokołów odbioru są:
   - …… tel. ……, e-mail ……, - …… tel. ……, e-mail …… .
2. Ze strony Wykonawcy, osobą odpowiedzialną za realizację Umowy oraz upoważnionymi do kontaktów jest:
   - …… tel. ……, e-mail …… .
3. Zmiana osób i danych wskazanych w ust. 1 i 2 nie wymaga zawarcia aneksu do Umowy i dla swej skuteczności wymaga pisemnego powiadomienia drugiej Strony.

§ 5 Obowiązki Wykonawcy

1. Wykonawca oświadcza, że posiada wszelkie niezbędne kwalifikacje, uprawnienia, doświadczenie i środki materialne oraz urządzenia niezbędne do wykonania Umowy.
2. Wykonawca zobowiązuje się do wykonania Przedmiotu Umowy zgodnie z parametrami i wymaganiami określonymi w Załączniku nr 1 do Umowy.
3. Wykonawca ponosi całkowitą odpowiedzialność za skutki działania lub zaniechania osób, przy udziale których lub z pomocą których realizuje niniejszą Umowę.
4. Wykonawca zobowiązany jest wykonać Umowę z zachowaniem należytej staranności wymaganej od przedsiębiorców świadczących na terytorium Rzeczypospolitej Polskiej usługi szkoleniowe.
5. Wykonawca ponosi całkowitą odpowiedzialność za własne działania lub zaniechania związane z realizacją Umowy, chyba że szkoda nastąpiła wskutek siły wyższej albo wyłącznie z winy Zamawiającego lub osoby trzeciej.

6. Wykonawca oświadcza, że wszystkie dostarczone materiały szkoleniowe stanowią jego wyłączną własność i nie są obciążone prawami osób trzecich.
7. Przeniesienie przez Wykonawcę jakichkolwiek praw lub zobowiązań związanych z wykonaniem Umowy na osobę trzecią wymaga pisemnej zgody Zamawiającego pod rygorem nieważności.

§ 6 Odpowiedzialność za niewykonanie lub nienależyte wykonanie Umowy

1. Wykonawca zapłaci Zamawiającemu karę umowną:
   1) za odstąpienie Wykonawcy od Umowy z przyczyn niezależnych od Zamawiającego albo w przypadku odstąpienia przez Zamawiającego od Umowy z przyczyn leżących po stronie Wykonawcy – w wysokości 20% całkowitego wynagrodzenia brutto określonego w § 3 ust. 1,
   2) w razie opóźnienia w wykonaniu przedmiotu umowy w terminie określonym w § 2 ust. 2 lub w § 2 ust. 3 - w wysokości 0,5% całkowitego wynagrodzenia brutto określonego w § 3 ust. 1 za każdy dzień opóźnienia,
   3) w przypadku ujawnienia jakiejkolwiek informacji lub innego naruszenia bezpieczeństwa informacji w okresie obowiązywania Umowy lub po wygaśnięciu lub rozwiązaniu Umowy – w wysokości 10% całkowitego wynagrodzenia brutto określonego w § 3 ust. 1 za każdy stwierdzony przypadek ujawnienia informacji lub innego naruszenia bezpieczeństwa informacji.
2. Zamawiający ma prawo na zasadach ogólnych dochodzić odszkodowania przenoszącego wysokość zastrzeżonych kary umownej.
3. Kary umowne mogą być naliczane niezależnie i podlegają sumowaniu.
4. Strony ustalają, iż naliczona przez Zamawiającego kara umowna może być przez niego potrącona z wynagrodzenia należnego Wykonawcy, wskazanego w § 3 ust. 1, na co niniejszym Wykonawca wyraża nieodwołalną zgodę.

§ 7 Zmiany umowy

Wszelkie zmiany Umowy, jej uzupełnienie lub rozwiązanie za zgodą obu stron, jak również odstąpienie od niej albo za jej wypowiedzenie wymaga zachowania formy pisemnej, pod rygorem nieważności.

§ 8 Odstąpienie od Umowy

1. Zamawiający może odstąpić od części lub całości Umowy w przypadkach określonych w przepisach obowiązującego prawa, w szczególności Kodeksu cywilnego.
2. Jeżeli Wykonawca opóźnia się z rozpoczęciem lub zakończeniem wykonania Umowy tak dalece, że nie jest prawdopodobne, żeby zdołał ją ukończyć w czasie umówionym, Zamawiający może, bez wyznaczenia terminu dodatkowego, od Umowy odstąpić jeszcze przed upływem terminu wykonania Umowy.
3. Zamawiający może odstąpić od Umowy, z przyczyn leżących po stronie Wykonawcy, w przypadku:
   1) złożenia wniosku o ogłoszenie upadłości lub otwarcia likwidacji Wykonawcy,
   2) zmiany formy organizacyjnej Wykonawcy, utrudniającej wykonanie Umowy, pod warunkiem, że nowy Wykonawca nie spełnia warunków udziału w postępowaniu, zachodzą wobec niego podstawy wykluczenia oraz pociąga to za sobą inne istotne zmiany Umowy - w ciągu 14 dni od dnia powzięcia wiadomości o takiej okoliczności.

4. Zamawiający może odstąpić od Umowy w przypadku zaistnienia istotnej zmiany okoliczności powodującej, że wykonanie Umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia Umowy, w ciągu 30 dni od dnia powzięcia wiadomości o tej okoliczności.
5. W przypadku odstąpienia od Umowy określonego w ust. 3 i 4 Wykonawca może żądać jedynie wynagrodzenia należnego mu z tytułu faktycznego wykonania części Umowy.
6. Odstąpienie od Umowy następuje w formie pisemnej pod rygorem nieważności, ze wskazaniem przyczyny odstąpienia.
7. Skorzystanie z prawa odstąpienia od Umowy nie znosi odpowiedzialności z tytułu zastrzeżonych w niej kar umownych i nie wyłącza uprawnienia do ich dochodzenia.

§ 9 Postanowienia końcowe

1. Prawem właściwym dla Umowy jest prawo polskie.
2. Żadna ze Stron Umowy nie może przenieść praw i obowiązków wynikających z niniejszej Umowy na osobę trzecią bez uprzedniego uzyskania zgody drugiej Strony, wyrażonej w formie pisemnej pod rygorem nieważności.
3. Sądem właściwym do rozstrzygnięcia sporów wynikłych z realizacji postanowień niniejszej Umowy będzie sąd miejscowo właściwy dla siedziby Zamawiającego.
4. Umowę sporządzono w trzech jednobrzmiących egzemplarzach, w tym dwa egzemplarze dla Zamawiającego i jeden dla Wykonawcy.

ZAMAWIAJĄCY **WYKONAWCA**

Załączniki:
Załącznik nr 1 – Opis Przedmiotu Zamówienia
Załącznik nr 2 – Wzór Protokołu odbioru szkolenia
Załącznik nr 3 – Wzór Protokołu odbioru egzaminu

Załącznik nr 1 do umowy nr … z dnia ……

Opis przedmiotu zamówienia I. Przedmiot zamówienia:

Przeprowadzenie szkoleń z zakresu egzaminu CompTIA Security+ (SY0-601) oraz organizacja egzaminu certyfikacyjnego.

II. Termin wykonania zamówienia:

Od dnia zawarcia umowy do dnia 20 grudnia 2021 roku.

III. Zakres i wymagania szczegółowe CompTIA Security+ (SY0-601):

6. Szkolenia i egzamin zostaną przeprowadzone do 20 grudnia 2021 roku.
7. W szkoleniu i egzaminach uczestniczyć będzie pięciu pracowników Zamawiającego.
8. Każdy uczestnik otrzyma dokument poświadczający ukończenie szkolenia.
9. Szkolenia i egzaminy muszą zostać przeprowadzone w języku polskim lub angielskim.
10. Wykonawca zobowiązuje się do zaproponowania co najmniej jednego terminu szkolenia do wyboru przez Zamawiającego.
11. Zakres merytoryczny szkolenia przygotowującego do egzaminu SY0-601 musi obejmować wszystkie tematy wyszczególnione w dokumencie „CompTIA Security+ Certification Exam Objectives", dostępnym na oficjalnej stronie CompTIA, to jest:
    a. 1.1 – Phishing, Smishing, Vishing, Spam, SpamoverInternetmessaging (SPIM) Spearphishing, Dumpsterdiving, Shouldersurfing, Pharming, Tailgating, Elicitinginformation, Whaling, Prepending, Identityfraud, Invoicescams, Credentialharvesting, Reconnaissance, Hoax, Impersonation, Wateringholeattack, Typosquatting, Pretexting, Influencecampaigns Hybridwarfare, Socialmedia, Principles(reasonsforeffectiveness) Authority Intimidation Consensus Scarcity Familiarity Trust Urgency;
    b. 1.2 – Malware, Ransomware, Trojans, Worms, Potentially unwanted programs (PUPs), Fileless virus, Command and control, Bots, Cryptomalware, Logic bombs, Spyware, Keyloggers, Remote access Trojan (RAT), Rootkit, Backdoor, Password attacks, Spraying, Dictionary, Brute force, Offline, Online, Rainbow tables, Plaintext/unencrypted, Physical attacks, Malicious universal, serial bus (USB) cable, Malicious flash drive, Card cloning, Skimming, Adversarial artificial intelligence (AI), Tainted training data for machine learning(ML),Security of machine learning algorithms, Supply-chain attacks, Cloud-based vs. on-premises attacks, Cryptographic attacks, Birthday, Collision, Downgrade;
    c. 1.3 – Privilege escalation, Cross-site scripting, Injections, Structured query language (SQL) Dynamic link library (DLL), Lightweight directory access protocol (LDAP), Extensible markup language (XML), Pointer/object dereference, Directory traversal, Buffer overflows, Race conditions Time of check/time of use, Error handling, Improper input handling, Replay attack, Session replays, Integer overflow, Request forgeries Server-side Client-side Cross-site, Application programming interface (API) attacks, Resource exhaustion, Memoryleak, Secure socket slayer (SSL) stripping, Driver manipulation, Shimming, Refactoring, Pass the hash;
    d. 1.4 – Wireless, Evil twin, Rogue access point, Bluesnarfing, Bluejacking, Disassociation, Jamming, Radio frequency identifier (RFID), Near-field

communication (NFC), Initialization vector (IV), Man-in-the-middle, Man-in-thebrowser, Layer 2 attacks, Address resolution protocol (ARP) poisoning, Media access control (MAC) flooding, MAC cloning, Domain name system (DNS), Domain hijacking, DNS poisoning, Universal resource locator (URL) redirection, Domain reputation, Distributed denial-of-service (DDoS), Network, Application, Operational technology (OT), Malicious code or script execution, PowerShell, Python, Bash, Macros, Virtual Basic for Applications (VBA);

e. 1.5 – Actors and threats, Advanced persistent threat (APT), Insider threats, State actors, Hacktivists, Script kiddies, Criminal syndicates, Hackers, White hat, Black hat, Gray hat, Shadow IT, Competitors, Attributes of actors,Internal/external, Level of sophistication/capability, Resources/funding, Intent/motivation, Vectors, Direct access, Wireless, Email, Supply chain, Social media, Removable media, Cloud, Threat intelligence sources, Open source intelligence (OSINT), Closed/proprietary, Vulnerability databases, Public/private information sharing centers, Dark web, Indicators of compromise, Automated indicator sharing (AIS), Structured Threat Information eXpression (STIX)/Trusted Automated eXchange of Indicator Information (TAXII), Predictive analysis, Threat maps, File/code repositories, Research sources, Vendor websites, Vulnerability feeds, Conferences, Academic journals, Request for comments (RFC), Local industry groups, Social media, Threat feeds -Adversary tactics, techniques and procedures (TTP);

f. 1.6 – Cloud-based vs on-premises vulnerabilities, Zero-day, Weak configurations, Open permissions, Unsecure root accounts, Errors, Weak encryption, Unsecure protocols, Default settings, Open ports and services, Third-party risks, Vendor management, System integration, Lack of vendor support, Supply chain, Outsourced code development, Data storage, Improper or weak patch management, Firmware, Operating system (OS), Applications, Legacy platforms, Impacts, Data loss, Data breaches, Data exfiltration, Identity theft, Financial, Reputation, Availability loss;

g. 1.7 - Threat hunting, Intelligence fusion, Threat feeds, Advisories and bulletins, Maneuver Vulnerability scans, False positives, False negatives, Log reviews, Credentialed vs. non-credentialed, Intrusive vs. non-intrusive, Application, Web application, Network, Common Vulnerabilities and Exposures (CVE)/Common,Vulnerability Scoring System (CVSS), Configuration review, Syslog/Security information and event management (SIEM), Review reports, Packet capture, Data inputs, User behavior analysis, Sentiment analysis, Security monitoring, Log aggregation, Log collector, Security orchestration, automation, and response (SOAR);

h. 1.8 - Penetration testing, White-box, Black-box, Gray-box, Rules of engagement, Lateral movement, Privilege escalation, Persistence, Cleanup, Bug bounty, Pivoting, Passive and active reconnaissance, Drones/unmanned aerial vehicle (UAV), War flying, War driving, Footprinting, OSINT, Exercise types, Red-team, Blue-team, White-team, Purple-team;

i. 2.1 Configuration management, Diagrams, Baseline configuration, Standard naming conventions, Internet protocol (IP) schema, Data sovereignty, Data protection, Data loss prevention (DLP), Masking, Encryption, At rest, In transit/motion, In processing, Tokenization, Rights management, Hardware security module (HSM), Geographical considerations, Cloud access security broker (CASB), Response and recovery

controls, Secure Sockets Layer (SSL)/Transport Layer Security (TLS) inspection, Hashing, API considerations, Site resiliency, Hot site, Cold site, Warm site, Deception and disruption, Honeypots, Honeyfiles, Honeynets, Fake telemetry, DNS sinkhole;

j. 2.2 – Cloud models, Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS), Anything as a service (XaaS), Public, Community, Private, Hybrid Cloud service providers, Managed service provider (MSP), managed security service provider (MSSP), On-premises vs. off-premises Fog computing Edge computing Thin client Containers Microservices/API, Infrastructure as code, Software-defined networking (SDN), Software-defined visibility (SDV) Serverless architecture Services integration Resource policies Transit gateway Virtualization, Virtual machine (VM) sprawl avoidance, VM escape protection;

k. 2.3 – Environment, Development, Test, Staging, Production, Quality assurance (QA) Provisioning and deprovisioning Integrity measurement Secure coding techniques, Normalization, Stored procedures, Obfuscation/camouflage, Code reuse/dead code, Server-side vs. client-side execution and validation, Memory management, Use of third-party libraries and software development kits (SDKs), Data exposure Open Web Application Security Project (OWASP) Software diversity, Compiler , Binary, Automation/scripting, Automated courses of action, Continuous monitoring, Continuous validation, Continuous integration, Continuous delivery, Continuous deployment Elasticity Scalability Version control;

l. 2.4 – Authentication methods, Directory services, Federation, Attestation, Technologies , Time-based one- time password (TOTP) , HMAC-based one-time password (HOTP) , Short message service (SMS) , Token key , Static codes , Authentication applications , Push notifications , Phone call, Smart card authentication, Biometrics, Fingerprint, Retina, Iris, Facial, Voice, Vein, Gait analysis, Efficacy rates, False acceptance, False rejection, Crossover error rate, Multifactor authentication (MFA) factors and attributes, Factors , Something you know , Something you have , Something you are, Attributes , Somewhere you are , Something you can do , Something you exhibit , Someone you know Authentication, authorization, and accounting (AAA) Cloud vs. on-premises requirements;

m. 2.5 – Redundancy, Geographic dispersal, Disk , Redundant array of inexpensive disks (RAID) levels , Multipath, Network , Load balancers , Network interface card (NIC) teaming, Power, Uninterruptible power supply (UPS), Generator, Dual supply, Managed power distribution units (PDUs), Replication, Storage area network, VM, On-premises vs. cloud, Backup types, Full, Incremental, Snapshot, Differential, Tape, Disk, Copy, Network-attached storage (NAS), Storage area network, Cloud, Image, Online vs. offline, Offsite storage, Distance considerations, Non-persistence, Revert to known state, Last known-good configuration, Live boot media, High availability, Scalability, Restoration order, Diversity, Technologies, Vendors, Crypto, Controls;

n. 2.6 – Embedded systems, Raspberry Pi, Field-programmable gate array (FPGA), Arduino, Supervisory control and data acquisition (SCADA)/industrial control system (ICS), Facilities, Industrial, Manufacturing, Energy, Logistics, Internet of Things (IoT), Sensors, Smart devices, Wearables, Facility automation, Weak defaults, Specialized, Medical systems, Vehicles, Aircraft, Smart meters, Voice over IP (VoIP), Heating, ventilation, air conditioning (HVAC), Drones/AVs, Multifunction printer (MFP), Real-time operating system (RTOS), Surveillance systems, System on chip (SoC),

Communication considerations, 5G, Narrow-band, Baseband radio, Subscriber identity module (SIM) cards, Zigbee, Constraints, Power, Compute, Network, Crypto, Inability to patch, Authentication, Range, Cost, Implied trust;

o. 2.7 - Bollards/barricades, Mantraps, Badges, Alarms, Signage, Cameras, Motion recognition, Object detection, Closed-circuit television (CCTV), Industrial camouflage, Personnel, Guards, Robot sentries, Reception, Two-person integrity/control, Locks, Biometrics, Electronic, Physical, Cable locks, USB data blocker, Lighting, Fencing, Fire suppression, Sensors, Motion detection, Noise detection, Proximity reader, Moisture detection, Cards, Temperature, Drones/UAV, Visitor logs, Faraday cages, Air gap, Demilitarized zone (DMZ), Protected cable distribution, Secure areas, Air gap, Vault, Safe, Hot aisle, Cold aisle, Secure data destruction, Burning, Shredding, Pulping, Pulverizing, Degaussing, Third-party solutions

p. 2.8 - Digital signatures, Key length, Key stretching, Salting, Hashing, Key exchange, Elliptic-curve cryptography, Perfect forward secrecy, Quantum, Communications, Computing, Post-quantum, Ephemeral, Modes of operation, Authenticated, Unauthenticated, Counter, Blockchain, Public ledgers, Cipher suites, Stream, Block, Symmetric vs. asymmetric, Lightweight cryptography, Steganography, Audio, Video, Image, Homomorphic encryption, Common use cases, Low power devices, Low latency, High resiliency, Supporting confidentiality, Supporting integrity, Supporting obfuscation, Supporting authentication, Supporting non-repudiation, Resource vs. security constraints, Limitations, Speed, Size, Weak keys, Time, Longevity, Predictability, Reuse, Entropy, Computational overheads, Resource vs. security constraints;

q. 3.1 – Protocols, Domain Name System, Security Extension (DNSSEC), SSH, Secure/Multipurpose Internet, Mail Extensions (S/MIME), Secure Real-time Protocol (SRTP), Lightweight Directory Access, Protocol Over SSL (LDAPS), File Transfer Protocol, Secure (FTPS), SSH File Transfer Protocol (SFTP), Simple Network Management,Protocol, version 3 (SNMPv3), Hypertext transfer protocol, over SSL/TLS (HTTPS), IPSec , Authentication header (AH)/,, Encapsulating Security,,Payloads (ESP) , Tunnel/transport, Secure Post Office Protocol (POP)/, Internet Message Access Protocol (IMAP) , Use cases, Voice and video, Time synchronization, Email and web, File transfer, Directory services, Remote access, Domain name resolution, Routing and switching, Network address allocation,
Subscription services;

r. 3.2 – ,Endpoint protection, Antivirus, Anti-malware, Endpoint detection and response (EDR), DLP, Next-generation firewall (NGFW), Host-based intrusion prevention system (HIPS), Host-based intrusion detection system (HIDS), Hostbased firewall , Boot integrity, Boot security/Unified Extensible, Firmware Interface (UEFI), Measured boot, Boot attestation , Database, Tokenization, Salting, Hashing ,
Application security, Input validations, Secure cookies, Hypertext Transfer Protocol (HTTP) headers, Code signing, Whitelisting, Blacklisting, Secure coding practices, Static code analysis , Manual code review, Dynamic code analysis, Fuzzing , Hardening, Open ports and services, Registry, Disk encryption, OS, Patch

management , Third-party updates , Auto-update , Self-encrypting drive (SED)/ fulldisk encryption (FDE), Opal , Hardware root of trust , Trusted Platform Module (TPM) , Sandboxing;

s. 3.3 – Load balancing, Active/active, Active/passive, Scheduling, Virtual IP, Persistence, Network segmentation, Virtual local area network (VLAN), DMZ, Eastwest traffic, Extranet, Intranet, Zero Trust, Virtual private network (VPN), Alwayson, Split tunnel vs. full tunnel, Remote access vs. site-to-site, IPSec, SSL/TLS, HTML5, Layer 2 tunneling protocol (L2TP), DNS, Network access control (NAC), Agent and agentless, Out-of-band management, Port security, Broadcast storm prevention, Bridge Protocol Data Unit (BPDU) guard, Loop prevention, Dynamic Host Configuration Protocol (DHCP) snooping, Media access control (MAC) filtering, Network appliances, Jump servers, Proxy servers , Forward , Reverse, Networkbased intrusion detection system (NIDS)/network-based intrusion prevention system (NIPS) , Signature-based , Heuristic/behavior , Anomaly , Inline vs. passive, HSM, Sensors, Collectors, Aggregators, Firewalls , Web application firewall (WAF), NGFW , Stateful , Stateless , Unified threat management (UTM) , Network address translation (NAT) gateway , Content/URL filter , Open-source vs. proprietary , Hardware vs. software , Appliance vs. host-based vs. virtual, Access control list (ACL), Route security, Quality of service (QoS), Implications of IPv6, Port spanning/port mirroring, Port taps, Monitoring services, File integrity monitors;

t. 3.4 – Cryptographic protocols, WiFi protected access II (WPA2), WiFi protected access III (WPA3), Counter-mode/CBC-MAC protocol (CCMP), Simultaneous Authentication of Equals (SAE) , Authentication protocols, Extensible Authentication Protocol (EAP), Protected Extensible Application Protocol (PEAP), EAP-FAST, EAPTLS, EAP-TTLS, IEEE 802.1X, Remote Authentication Dial-in User Service (RADIUS) Federation , Methods, Pre-shared key (PSK) vs. Enterprise vs. Open, WiFi Protected Setup (WPS), Captive portals , Installation considerations, Site surveys, Heat maps, WiFi analyzers, Channel overlays, Wireless access point (WAP) placement, Controller and access point security;

u. 3.5 – , Connection methods and receivers, Cellular, WiFi, Bluetooth, NFC, Infrared, USB, Point-to-point, Point-to-multipoint, Global Positioning System (GPS), RFID , Mobile device management (MDM), Application management, Content management, Remote wipe, Geofencing, Geolocation, Screen locks, Push notifications, Passwords and pins, Biometrics, Context-aware authentication, Containerization, Storage segmentation, Full device encryption , Mobile devices, MicroSD HSM, MDM/Unified Endpoint Management (UEM), Mobile application management (MAM), SEAndroid , Enforcement and monitoring of:, Third-party application stores, Rooting/jailbreaking, Sideloading, Custom firmware, Carrier unlocking, Firmware over-the-air (OTA) updates, Camera use, SMS/Multimedia Messaging Service (MMS)/Rich communication services (RCS), External media, USB On-The-Go (USB OTG), Recording microphone, GPS tagging, WiFi direct/ad hoc, Tethering, Hotspot, Payment methods , Deployment models, Bring your own device (BYOD), Corporate-owned personally enabled (COPE), Choose your own device (CYOD), Corporate-owned, Virtual desktop infrastructure (VDI);

v. 3.6 – Cloud security controls, High availability across zones, Resource policies, Secrets management, Integration and auditing, Storage , Permissions , Encryption ,

Replication , High availability, Network, Virtual networks, Public and private subnets, Segmentation, API inspection and integration, Compute , Security groups , Dynamic resource allocation , Instance awareness , Virtual private cloud (VPC) endpoint , Container security, Solutions, CASB, Application security, Nextgeneration Secure Web Gateway (SWG), Firewall considerations in a cloud environment , Cost , Need for segmentation , Open Systems Interconnection (OSI) layers , Cloud native controls vs. third-party solutions;

w. 3.7 - Identity, Identity provider (IdP), Attributes, Certificates, Tokens, SSH keys, Smart cards , Account types, User account, Shared and generic accounts/credentials, Guest accounts, Service accounts , Account policies, Password complexity, Password history, Password reuse, Time of day, Network location, Geofencing, Geotagging, Geolocation, Time-based logins, Access policies, Account permissions, Account audits, Impossible travel time/risky login, Lockout, Disablement;

x. 3.8 - Authentication management, Password keys, Password vaults, TPM, HSM, Knowledge-based authentication , Authentication, EAP, Challenge Handshake Authentication Protocol (CHAP), Password Authentication Protocol (PAP), 802.1X, RADIUS, Single sign-on (SSO), Security Assertions Markup Language (SAML), Terminal Access Controller Access Control System Plus (TACACS+), OAuth, OpenID, Kerberos , Access control schemes, Attribute-based access control (ABAC), Rolebased access control, Rule-based access control, MAC, Discretionary access control (DAC), Conditional access, Privilege access management, Filesystem permission;

y. 3.9 – Public key infrastructure (PKI), Key management, Certificate authority (CA), Intermediate CA, Registration authority (RA), Certificate revocation list (CRL), Certificate attributes, Online Certificate Status Protocol (OCSP), Certificate signing request (CSR), CN, Subject alternative name, Expiration, Types of certificates, Wildcard, Subject alternative name, Code signing, Self-signed, Machine/computer, Email, User, Root, Domain validation, Extended validation , Certificate formats, Distinguished encoding rules (DER), Privacy enhanced mail (PEM), Personal information exchange (PFX), .cer, P12, P7B , Concepts, Online vs. offline CA, Stapling, Pinning, Trust model, Key escrow , Certificate chaining;

4.1 – Network reconnaissance and discovery, tracert/traceroute, nslookup/dig, ipconfig/ifconfig, nmap, ping/pathping, hping, netstat, netcat, IP scanners, arp, route, curl, the harvester, sn1per, scanless, dnsenum, Nessus, Cuckoo, File manipulation, head, tail, cat, grep, chmod, logger, Shell and script environments, SSH, PowerShell, Python, OpenSSL, Packet capture and replay, Tcpreplay, Tcpdump, Wireshark, Forensics, dd, Memdump, WinHex, FTK imager, Autopsy, Exploitation frameworks, Password crackers, Data sanitization;

z. 4.2 – Incident response plans, Incident response process, Preparation, Identification, Containment, Eradication, Recovery, Lessons learned, Exercises, Tabletop, Walkthroughs, Simulations, Attack frameworks, MITRE ATT&CK, The Diamond Model of Intrusion Analysis, Cyber Kill Chain, Stakeholder management, Communication plan, Disaster recovery plan, Business continuity plan, Continuity of operations planning (COOP), Incident response team, Retention policies;

aa. 4.3 – Vulnerability scan output, SIEM dashboards, Sensor, Sensitivity, Trends, Alerts, Correlation, Log files, Network, System, Application, Security, Web, DNS, Authentication, Dump files, VoIP and call managers, Session Initiation Protocol (SIP) traffic, syslog/rsyslog/syslog-ng, journalctl, nxlog, Retention, Bandwidth monitors, Metadata, Email, Mobile, Web, File, Netflow/sflow, Echo, IPfix, Protocol analyzer output;

bb. 4.4 – Reconfigure endpoint security solutions, Application whitelisting, Application blacklisting, Quarantine, Configuration changes, Firewall rules, MDM, DLP, Content filter/URL filter, Update or revoke certificates, Isolation, Containment,

Segmentation, SOAR, Runbooks, Playbook; cc. 4.5 - Documentation/evidence, Legal hold, Video, Admissibility, Chain of custody, Timelines of sequence of events , Time stamps , Time offset, Tags, Reports, Event logs, Interviews, Acquisition, Order of volatility, Disk, Random-access memory

(RAM), Swap/pagefile, OS, Device, Firmware, Snapshot, Cache, Network, Artifacts, On-premises vs. cloud, Right-to-audit clauses, Regulatory/jurisdiction, Data breach notification laws , Integrity, Hashing, Checksums, Provenance , Preservation , Ediscovery , Data recovery , Non-repudiation , Strategic intelligence/ counterintelligence;

dd. 5.1 – Category, Managerial, Operational, Technical, Control type, Preventative,

Detective, Corrective, Deterrent, Compensating, Physical; ee. 5.2 – , Regulations, standards, and legislation, General Data Protection Regulation (GDPR), National, territory, or state laws, Payment Card Industry Data Security Standard (PCI DSS), Key frameworks, Center for Internet Security (CIS), National Institute of Standards and Technology (NIST) RMF/CSF, International Organization for Standardization (ISO) 27001/27002/27701/31000, SSAE SOC 2 Type I/II, Cloud security alliance, Cloud control matrix, Reference architecture, Benchmarks /secure configuration guides, Platform/vendor-specific guides, Web server, OS, Application server, Network infrastructure devices;

ff. 5.3 – Personnel, Acceptable use policy, Job rotation, Mandatory vacation, Separation of duties, Least privilege, Clean desk space, Background checks, Nondisclosure agreement (NDA), Social media analysis, Onboarding, Offboarding, User training, Gamification, Capture the flag, Phishing campaigns , Phishing simulations, Computer-based training (CBT), Role-based training Diversity of training techniques Third-party risk management, Vendors, Supply chain, Business partners, Service level agreement (SLA), Memorandum of understanding (MOU), Measurement systems analysis (MSA), Business partnership agreement (BPA), End of life (EOL), End of service (EOS), NDA Data, Classification, Governance, Retention Credential policies, Personnel, Third-party, Devices, Service accounts, Administrator/root accounts Organizational policies, Change management, Change control, Asset management;

gg. 5.4 – , Risk types, External, Internal, Legacy systems, Multiparty, IP theft, Software compliance/licensing , Risk management strategies, Acceptance, Avoidance, Transference , Cybersecurity insurance, Mitigation , Risk analysis, Risk register, Risk matrix/heat map, Risk control assessment, Risk control self-assessment, Risk awareness, Inherent risk, Residual risk, Control risk, Risk appetite, Regulations that affect risk posture, Risk assessment types , Qualitative , Quantitative, Likelihood of occurrence, Impact, Asset value, Single loss expectancy (SLE), Annualized loss

expectancy (ALE), Annualized rate of occurrence (ARO), Disasters, Environmental, Person-made, Internal vs. external , Business impact analysis, Recovery time objective (RTO), Recovery point objective (RPO), Mean time to repair (MTTR), Mean time between failures (MTBF), Functional recovery plans, Single point of failure, Disaster recovery plan (DRP), Mission essential functions, Identification of critical systems, Site risk assessment;

hh. 5.5 – Organizational consequences of privacy breaches, Reputation damage, Identity theft, Fines, IP theft, Notifications of breaches, Escalation, Public notifications and disclosures, Data types, Classifications, Public, Private, Sensitive, Confidential, Critical, Proprietary, Personally identifiable information (PII), Health information, Financial information, Government data, Customer data, Privacy enhancing technologies, Data minimization, Data masking, Tokenization, Anonymization, Pseudo-anonymization, Roles and responsibilities, Data owners, Data controller, Data processor, Data custodian/steward, Data protection officer (DPO), Information life cycle, Impact assessment, Terms of agreement, Privacy notic;

12. Podmiot przeprowadzający szkolenie przygotowujące do egzaminu SY0-601 posiada status autoryzowanego przez CompTIA partnera szkoleniowego w zakresie przygotowania do egzaminu CompTIA Security+ (SY0-601) lub szkolenie zostanie przeprowadzone przez trenera z certyfikatem Comptia Sec+, uprawnionym do przeprowadzania szkolenia.

IV. Warunki przeprowadzania szkoleń

1. Wykonawca, przygotuje harmonogram szkolenia oraz program szkolenia i dostarczy je w terminie nie później niż 7 dni roboczych przed dniem rozpoczęcia szkolenia do akceptacji przez Zamawiającego. Harmonogram zajęć powinien zawierać informacje dotyczące czasu i miejsca realizacji danego szkolenia.
2. Wykonawca przygotuje i zapewni materiały szkoleniowe dla każdego uczestnika szkolenia, pozwalające na samodzielną edukację z zakresu tematyki szkolenia (np. opracowania, wydruki materiałów szkoleniowych).
3. Komplet materiałów szkoleniowych dla każdego uczestnika szkolenia obejmuje papierową wersję materiałów szkoleniowych. Zamawiający dopuszcza dostarczenie materiałów w formie elektronicznej, np. dokumenty w standardzie PDF, w miejsce materiałów papierowych.
4. Wykonawca dostarczy uczestnikom szkolenia ww. materiały szkoleniowe najpóźniej w dniu rozpoczęcia szkolenia.
5. Koszty opracowania, powielenia i transportu materiałów szkoleniowych ponosi Wykonawca.
6. Zamawiający dopuszcza przeprowadzenie szkolenia z wykorzystaniem narzędzi umożliwiających wideokonferencję na poniższych warunkach:
   a. Oprogramowanie wykorzystane do udostępnienia ekranu komputera prowadzącego, obrazu oraz dźwięku z sali szkoleniowej zostanie udostępnione uczestnikom szkolenia bez ponoszenia przez Zamawiającego dodatkowych kosztów. Wykorzystane oprogramowanie będzie pochodzić z legalnego źródła oraz sposób użycia nie może naruszać warunków licencyjnych, na jakich oprogramowanie zostało udostępnione.
   b. Wykorzystane oprogramowanie musi umożliwiać uczestnikom szkolenia zadawanie pytań i zgłaszanie wątpliwości w czasie rzeczywistym.
   c. Sposób prowadzenia szkolenia przez prowadzącego musi umożliwiać uczestnikom zadawanie pytań i zgłaszanie wątpliwości w czasie rzeczywistym.

7. Harmonogram szkolenia musi uwzględniać czas na przerwy regeneracyjne oraz przerwę obiadową w następującej ilości i o następującym czasie trwania:
    a. Minimum jedna przerwa regeneracyjna o przynajmniej 10 minutowym czasie trwania pomiędzy godziną 8:00 a 11:00;
    b. Jedna co najmniej 30 minutowa przerwa obiadowa pomiędzy godziną 12:30 a godziną 14:00;
    c. Minimum jedna przerwa regeneracyjna o przynajmniej 10 minutowym czasie trwania pomiędzy godziną 13:30 a 16:00.
8. Wykonawca nie jest zobowiązany do zapewnienia uczestnikom szkolenia wyżywienia.
9. Wykonawca w ramach otrzymanego wynagrodzenia zapewni uczestnikom szkolenia imienne certyfikaty potwierdzające ukończenie szkolenia i jego zakres

V. Warunki i wymagania dotyczące przeprowadzania egzaminów

1. Wykonawca zapewni na cele realizacji przedmiotu zamówienia bazę egzaminacyjną z odpowiednimi pomieszczeniami wraz z zapleczem do przeprowadzenia egzaminów dla osób dorosłych, tj. sale dostosowane do przeprowadzania egzaminów, dobrze oświetlone (światło dzienne i sztuczne), wentylowane (z dostępem do świeżego powietrza), posiadające odpowiednie warunki sanitarne, bezpieczeństwa i higieny pracy, wyposażone w akustyczne i jakościowe narzędzia i urządzenia, a także oprogramowanie i pomoce dydaktyczne niezbędne do wykonania zamówienia.
2. W pobliżu sali egzaminacyjnej (w tym samym budynku) powinny znajdować się łazienki z węzłem sanitarnym.
3. Egzamin zostanie przeprowadzony nie wcześniej niż 2 miesiące i nie później niż 5 miesięcy po zakończeniu szkolenia.
4. Egzamin odbędzie się w dzień powszedni od poniedziałku do piątku, w godzinach od 8:00 do 17:00.
5. Egzamin zostanie przeprowadzony na terenie Warszawy lub w formie zdalnej.
6. Do egzaminu przystąpi pięciu pracowników Zamawiającego, którzy ukończyli szkolenie.
7. Każdy uczestnik otrzyma dokument potwierdzający przystąpienie do egzaminu wraz z jego wynikami.
8. Egzamin będzie przeprowadzony w języku polskim lub angielskim.
9. Wykonawca zobowiązuje się do wskazania trzech terminów egzaminu do wyboru przez Zamawiającego.
10. Podmiot przeprowadzający egzamin CompTIA Security+ (SY0-601) musi posiadać status podmiotu egzaminującego autoryzowanego przez CompTIA.

Załącznik nr 2 do umowy nr … z dnia ……

Protokół odbioru szkolenia

Warszawa, dnia ……

Protokół z przeprowadzonego szkolenia CompTIA Security+ (SY0-601)

W dniach …… - …… odbyło się szkolenie z zakresu egzaminu CompTIA Security+ (SY0-601).

Plan szkolenia:

1. Dnia …:
    a. …
    b. …
    c. etc.
2. Dnia …:
    a. …
    b. …
    c. etc.
3. etc.

W szkoleniu udział wzięli:

1. Dnia …:
    a. …
    b. …
    c. etc.
2. Dnia …:
    a. …
    b. …
    c. etc.
3. etc.

…… ……

podpis osoby przeprowadzającej szkolenie podpis osoby odbierającej szkolenie

Załącznik nr 3 do umowy nr … z dnia ……

Protokół odbioru egzaminu

Warszawa, dnia ……

Protokół z przeprowadzonego egzaminu CompTIA Security+ SY0-601

W dniach …… - …… odbył się egzamin CompTIA Security+ SY0-601.

W egzaminie udział wzięli:

1. … 2.
… 3. …
4. …

…… ……

podpis osoby przeprowadzającej egzamin podpis osoby odbierającej egzamin

Załącznik nr 3
do zamówienia nr BC-II.252.1.2021

MINISTERSTWO SPRAWIEDLIWOŚCI
www.ms.gov.pl

FORMULARZ CENOWY

na realizację zamówienia - Przeprowadzenie szkolenia w zakresie certyfikacji CompTIA Security+

I. DANE DOTYCZĄCE OFERENTA:

Nazwa podmiotu	
Adres siedziby	
Numer NIP	
Numer REGON	
Telefon kontaktowy	
Adres e-mail	

II. CAŁKOWITA SZACOWANA WARTOŚĆ ZAMÓWIENIA:

…… zł. brutto

Słownie: ……

…… zł. netto

Słownie: ……

III. CAŁKOWITA SZACOWANA WARTOŚĆ ZAMÓWIENIA W INNYM WARIANCIE OSOBOWYM (CENA ZA JEDNĄ OSOBĘ):

…… zł. brutto

Słownie: ……

…… zł. netto

Słownie: ……

_____

Podpis osoby upoważnionej