AZU
Agencija za ugljikovodike

KLASA: 406-07/25-01/59
URBROJ: 405-02/01-25-3

Zagreb, 12. rujna 2025. godine

Predmet: Poziv na dostavu ponude u postupku jednostavne nabave za predmet nabave: **Savjetodavne usluge izrade dokumentacije u svrhu usklađivanja Agencije sa Zakonom o kibernetičkoj sigurnosti kroz provedbu mjera upravljanja kibernetičkim sigurnosnim rizicima.**

Temeljem članka 8. Pravilnika o nabavi roba i usluga temeljem postupka jednostavne nabave (KLASA: 400-09/17-01/02, UR.BROJ: 405-01/1-18-2) od 30. listopada 2018. godine Agencija za ugljikovodike (dalje u tekstu: AZU) objavljuje Poziv na dostavu ponuda za postupak jednostavne nabave: **Savjetodavne usluge izrade dokumentacije u svrhu usklađivanja Agencije sa Zakonom o kibernetičkoj sigurnosti kroz provedbu mjera upravljanja kibernetičkim sigurnosnim rizicima.**

Opis predmeta nabave:

Agencija za ugljikovodike (dalje u tekstu: Naručitelj) provodi usklađivanje sa Zakonom o kibernetičkoj sigurnosti („Narodne novine“, br. 14/2024; dalje u tekstu Zakon) sukladno provedenoj kategorizaciji i utvrđenoj razini kibernetičkih sigurnosnih rizika.

Predmetna Usluga usklađivanja s Zakonom obuhvaća slijedeće faze:

1. **Analiza utjecaja na poslovanje**
2. **Planiranje kontinuiteta poslovanja**
3. **Izrada plana oporavka poslovanja**
4. **Uspostava sustava upravljanja rizicima informacijske sigurnosti**
5. **Izrada dokumentacije usklađene sa Zakonom**
6. **Alat za upravljanje kibernetičkom sigurnošću i usklađenošću (vCISO)**

1. **Analiza utjecaja na poslovanje**

Analiza utjecaja na poslovanje mora obuhvatiti prepoznavanje svih ključnih poslovnih funkcija, procjenu i izražavanje gubitaka nastalih uslijed prekida rada, utvrđivanje dopuštenog trajanja zastoja te određivanje minimalnih resursa nužnih za obnovu kritičnih funkcija. Sve usklađeno sa Zakonom.

Isporuke koje se očekuju:

- Metodologija provedbe analize utjecaja na poslovanje,
- Ispunjeni upitnici analize utjecaja na poslovanje i
- Izvješće o analizi utjecaja na poslovanje.

2. **Planiranje kontinuiteta poslovanja**

Planiranje kontinuiteta poslovanja mora obuhvatiti izradu dogovorenih postupaka i procedura kojima se omogućuje odgovor na sigurnosni događaj, radi osiguranja nastavka kritičnih poslovnih funkcija unutar prihvatljivih razina nedostupnosti sustava. Krajnji rezultat navedenog procesa je Plan kontinuiteta poslovanja. Sve usklađeno sa Zakonom.

Isporuke koje se očekuju:

- Rezultati analize,
- Definirani timovi,
- Procjena resursa (kadrovski i financijski),
- Strategija kontinuiteta poslovanja i upravljanje kriznim situacijama,
- Izrada operativnih planova kontinuiteta poslovanja,
- Zapisnici nakon edukacije.

3. **Izrada plana oporavka poslovanja**

Planiranje nastavka poslovanja mora obuhvatiti aktivnosti vezane uz vraćanje kritičnih poslovnih funkcija nakon hitnog slučaja. Plan mora uključivati operativne procedure potrebne za osiguranje kontinuiteta ključnih funkcija tijekom hitnog slučaja ili prekida poslovanja. Sve usklađeno sa Zakonom.

Isporuke koje se očekuju:

- Planovi oporavka poslovanja nakon katastrofe sa procedurom za upravljanje kriznim situacijama,
- Planovi testiranja planova oporavka,
- Zapisnici testiranja planova oporavka.

4. **Uspostava sustava upravljanja rizicima informacijske sigurnosti**

Uspostava postupka upravljanja rizicima mora obuhvatiti definiranje kriterija za identifikaciju, analizu, evaluaciju, te postupak obrade i upravljanja rizicima informacijske sigurnosti, s ciljem kontinuiranog praćenja i održavanja prihvatljive razine rizika informacijske sigurnosti. Sve usklađeno sa Zakonom.

Isporuke koje se očekuju:

- Procedura za upravljanje rizicima informacijske sigurnosti,
- Metodologija procjene i obrade rizika informacijske sigurnosti,
- Izvješće o procjeni i obradi rizika informacijske sigurnosti.

5. **Izrada dokumentacije usklađene sa Zakonom**

Izrada dokumentacije mora obuhvatiti uspostavu krovne Politike informacijske sigurnosti usklađene s ISO/IEC 27001:2022, NIS2 direktivom te Zakonom o kibernetičkoj sigurnosti, kojom se definiraju opseg, ciljevi i načela sustava upravljanja informacijskom sigurnošću. Politika mora specificirati uloge i odgovornosti svih osoba uključenih u sustav upravljanja.

Politika informacijske sigurnosti mora dodatno osigurati provedbu kontrola informacijske sigurnosti.

Isporuke koje se očekuju:

- Definirane uloge i odgovornosti,
- Politika informacijske sigurnosti,
- Procedura za primjereno korištenje imovine,
- Pravilnik za klasifikaciju imovine,
- Primjer predloška popisa imovine,
- Prijedlog poboljšanja procedura vezanih za ljudske resurse i informacijsku sigurnost,
- Program podizanja svijesti,
- Prezentacija za podizanje svijesti za novozaposlene,
- Politika/procedura kontrole fizičkog i logičkog pristupa,
- Politika sigurnosti za odnose s dobavljačima i nadzor dobavljačkog lanca,
- Politika sigurnog razvoja i upravljanja informacijskim sustavima,
- Procedura za upravljanje promjenama,
- Politika sigurnog razvoja i upravljanja informacijskim sustavom,
- Politika korištenja kriptografskih kontrola,
- Procedura za odgovor na sigurnosne incidente,
- Nadzor kontrola informacijske sigurnosti,
- Plan i program revizije Sustava upravljanja informacijskom sigurnošću;
- Primjer izvješća o rezultatima revizije Sustava upravljanja informacijskom sigurnošću.

6. Alat za upravljanje kibernetičkom sigurnošću i usklađenošću (vCISO)

Korištenje alata za upravljanje kibernetičkom sigurnošću i usklađenošću mora obuhvatiti funkcionalnosti koje omogućuju učinkovito upravljanje kibernetičkom sigurnošću i usklađenošću putem automatizacije ključnih GRC (Governance, Risk, Compliance) procesa. Alat mora omogućiti procjenu sigurnosnog stanja, pružanje prilagođenih sigurnosnih smjernica te kontinuirano praćenje i izvještavanje, čime se smanjuje potreba za ručnim radom i povećava operativna učinkovitost.

Isporuke koje se očekuju:

- procjenu rizika i usklađenosti,
- stalno upravljanje, mjerenje i optimizaciju,
- skeniranje ranjivosti,
- analizu utjecaja na poslovanje,
- planove kontinuiteta poslovanja,

- procjenu rizika trećih strana,
- periodična izvješća,
- planove kibernetičke sigurnosti s prilagođenim politikama,
- prioritizirane zadatke sanacije nedostataka,
- praćenje procesa i pregled u stvarnom vremenu putem nadzorne ploče,
- uslugu ugovorenu na jednu (1) godinu,
- uspostavu vCISO rješenja,
- podršku za održavanje vCISO rješenja,
- inicijalnu obuku za upravljanje platformom, koja pokriva sve njezine module,
- pristup nadzornoj ploči u stvarnom vremenu.

Reference i stručni tim ponuditelja

Ponuditelj mora imati relevantno iskustvo i provjerljive reference na poslovima koji uključuju analizu utjecaja na poslovanje, planiranje kontinuiteta poslovanja, izradu plana oporavka poslovanja, uspostavu sustava upravljanja rizicima informacijske sigurnosti, izradu dokumentacije usklađene sa Zakonom o kibernetičkoj sigurnosti (ZKS) te implementaciju i korištenje alata za upravljanje kibernetičkom sigurnošću i usklađenošću (vCISO).

Tim ponuditelja mora se sastojati od najmanje 3 (slovima: tri) stručne osobe, pri čemu najmanje (slovima; dvije) moraju posjedovati međunarodno priznate certifikate iz područja kibernetičke sigurnosti i upravljanja rizicima i to:

- Certified Information Systems Security Professional (CISSP), koji izdaje ISC2 – International Information System Security Certification Consortium,
- Certified in Risk and Information Systems Control (CRISC), koji izdaje ISACA – Information Systems Audit and Control Association,
- Certified Information Security Manager (CISM), koji izdaje ISACA – Information Systems Audit and Control Association,
- Certified Information Systems Auditor (CISA), koji izdaje ISACA – Information Systems Audit and Control Association,
- Certified Cloud Security Professional (CCSP), koji izdaje ISC2 – International Information System Security Certification Consortium.

Način izvršenja Usluge:

Za izvršenje usluge koja je predmet jednostavne nabave sklopit će se Ugovor.

Dostava ponuda:

Molimo Vas da nam sukladno prethodno navedenom, dostavite Vašu ponudu u papirnatom pisanom obliku, u zatvorenoj omotnici na kojoj je naziv i adresa Naručitelja i nazivi i adresa Ponuditelja. Na vanjskom omotu mora biti adresa i oznaka slijedećeg izgleda:

AZU
Agencija za ugljikovodike

AGENCIJA ZA UGLJIKOVODIKE
Miramarska cesta 24
10 000 Zagreb

Ponuda za jednostavnu nabavu: **Savjetodavne usluge izrade dokumentacije u svrhu usklađivanja Agencije sa Zakonom o kibernetičkoj sigurnosti kroz provedbu mjera upravljanja kibernetičkim sigurnosnim rizicima**

„NE OTVARAJ"

Ponuda mora biti dostavljena Naručitelju najkasnije dana 22. rujna 2025. godine do 10:00 sati.

Vaša ponuda mora biti izražena u neto iznosu, a treba sadržavati ispunjen, potpisan i ovjeren:

1. Prilog 1 - Ponudbeni list
2. Prilog 2 - Troškovnik

Početak Ugovora: 1. listopada 2025. godine.

Trajanje Ugovora: 12 mjeseci.

Način plaćanja:

Plaćanje će se izvršavati po isporuci pojedinih faza usluge. Svaka faza mora biti verificirana i prihvaćena od strane Naručitelja prije izvršenja pripadajuće uplate. Faze usluge obuhvaćaju:

1. Analizu utjecaja na poslovanje,
2. Planiranje kontinuiteta poslovanja,
3. Izradu plana oporavka poslovanja,
4. Uspostavu sustava upravljanja rizicima informacijske sigurnosti,
5. Izradu dokumentacije usklađene sa Zakonom o kibernetičkoj sigurnosti (ZKS),
6. Implementaciju i korištenje alata za upravljanje kibernetičkom sigurnošću i usklađenošću (vCISO).

Sve faze isporuke moraju biti u skladu sa zahtjevima Naručitelja i potvrđene prije isplate.

Svaka od 6 (slovima: šest) faza isplaćuje se u jednakim novčanim iznosima, a ukupna cijena svih faza čini cjelokupnu ugovorenu vrijednost usluge.

Plaćanje po fazama isporuke izvršiti će se na poslovni račun odabranog ponuditelja na temelju ispostavljenih e-računa te potpisanog zapisnika o isporučenoj fazi isporuke u roku 15 (slovima: petnaest) dana od dana primitka e-računa.

AZU
Agencija za ugljikovodike

Rok isporuke:

Usluga će se isporučivati fazno, pri čemu će svaka faza biti verificirana i prihvaćena od strane naručitelja prije izvršenja pripadajuće uplate. Zadnja, završna faza usluge mora biti isporučena najkasnije 12 (slovima: dvanaest) mjeseci od datuma obostranog potpisa Ugovora, čime se osigurava cjelokupna isporuka svih faza unutar propisanog roka.

Mjesto izvršenja predmeta nabave:

Odabrani ponuditelj će usluge koje čine predmet nabave izvršavati u svojim poslovnim prostorima, u poslovnim prostorima Naručitelja te na drugim lokacijama ovisno o prirodi usluge i zahtjevima Naručitelja, a sve u skladu s opisom predmeta nabave. Prema potrebama Naručitelja, sastanci i druge aktivnosti u sklopu ovog predmeta nabave održavat će se u sjedištu Naručitelja.

Opcija ponude: 8 dana od krajnjeg roka za dostavu ponuda.

Kontakt osoba: Tomislav Gojčeta
Telefon: 01/6431-920
e-mail: tomislav.gojceta@azu.hr

S poštovanjem,

Agencija za ugljikovodike Miramarska 24, Zagreb

Marijan Krpan
predsjednik Uprave