31.

Na osnovu člana 21 stav 2 Zakona o zaključivanju i izvršavanju međunarodnih ugovora ("Službeni list CG", broj 77/08), Vlada Crne Gore na sjednici od 4. maja 2018. godine, donijela je

ODLUKA

O OBJAVLJIVANJU SPORAZUMA IZMEĐU VLADE CRNE GORE I VLADE SJEDINJENIH AMERIČKIH DRŽAVA U VEZI SA BEZBJEDNOSNIM MJERAMA ZA ZAŠTITU TAJNIH PODATAKA

("Službeni list Crne Gore - Međunarodni ugovori", br. 006/18 od 01.06.2018)

Član 1

Objavljuje se Sporazum između Vlade Crne Gore i Vlade Sjedinjenih Američkih Država u vezi sa bezbjednosnim mjerama za zaštitu tajnih podataka potpisan u Vašingtonu, 27. februara 2018. godine, u originalu na crnogorskom i engleskom jeziku.

Član 2

Tekst Sporazuma iz člana 1 ove odluke, u originalu na crnogorskom i engleskom jeziku glasi:

SPORAZUM

IZMEĐU VLADE CRNE GORE I VLADE SJEDINJENIH AMERIČKIH DRŽAVA U VEZI SA BEZBJEDNOSNIM MJERAMA ZA ZAŠTITU TAJNIH PODATAKA

PREAMBULA

Vlada Crne Gore ("Crna Gora") i Vlada Sjedinjenih Američkih Država ("Sjedinjene Države") (u daljem tekstu: "Strane", a pojedinačno: "Strana"),

Imajući u vidu da Strane sarađuju u oblastima koje uključuju, ali se ne ograničavaju isključivo na njih, spoljne poslove, odbranu, bezbjednost, vladavinu prava, nauku, industriju, i tehnologiju i

Imaju zajednički interes u zaštiti tajnih podataka koji su u povjerenju razmijenjeni između Strana,

Sporazumjele su se o sljedećem:

Član 1

- DEFINICIJE

U cilju ovog Sporazuma:

1. Tajni podaci: Podaci koje jedna Strana ustupa drugoj Strani, i koje je Strana koja ih ustupa označila stepenom tajnosti u svrhu zaštite nacionalne bezbjednosti i koji iz tih razloga zahtijevaju zaštitu od neovlašćenog otkrivanja. Podaci mogu biti usmeni, vizuelni, u elektronskoj ili papirnoj formi, ili u formi materijala, uključujući opremu ili tehnologiju.

2. Povjerljivi ugovor: Ugovor koji zahtijeva, ili će zahtijevati pristup, ili stvaranje tajnih podataka od strane Ugovarača ili njegovih zaposlenih u toku izvršavanja ugovora.

3. Ugovarač: Fizičko ili pravno lice, koje posjeduje poslovnu sposobnost za zaključivanje Ugovora, a koje je ugovorna strana Povjerljivog ugovora.

4. Dozvola za pristup tajnim podacima za pravno lice: dozvola koju izdaje Nacionalni bezbjednosni organ Strane, određen članom 4, za objekat Ugovarača koji je pod njegovom nadležnošću, koja potvrđuje da je objekat Ugovarača bezbjednosno provjeren do određenog stepena i da postoje odgovarajuće bezbjednosne mjere za čuvanje tajnih podataka određenog stepena tajnosti. Takva dozvola će potvrditi da će tajni podaci stepena tajnosti CONFIDENTIAL/POVJERLJIVO ili više biti zaštićeni od strane Ugovarača kome je izdata dozvola za pristup tajnim podacima za pravna lica, u skladu sa odredbama ovog Sporazuma i da će usklađenost biti pod nadzorom i kontrolom Nacionalnog bezbjednosnog organa. Dozvola za pristup tajnim podacima za pravna lica za Ugovarača koji izvršava Ugovor koji podrazumijeva samo prijem ili nastanak tajnih podataka označenih stepenom tajnosti INTERNO (RESTRICTED) se ne zahtijeva.

5. Dozvola za pristup tajnim podacima za fizičko lice:

a. Potvrda Nacionalnog bezbjednosnog organa Strane, određenog članom 4, da je lice zaposleno u državnim organima Strane ili Ugovarač koji je pod njenom nadležnošću ovlašćeno za pristup tajnim podacima do određenog stepena tajnosti.

b. Potvrda Nacionalnog bezbjednosnog organa Strane, određenog članom 4, da je lice koje ima državljanstvo te Strane ali treba da bude zaposleno od strane druge Strane, ili nekog od Ugovarača druge Strane, ovlašćeno za pristup tajnim podacima do određenog stepena tajnosti.

6. Potrebno je da zna: potvrda ovlašćenog lica koje posjeduje tajni podatak da mogući primalac tajnog podatka zahtijeva pristup određenom tajnom podatku u cilju izvršenja ili pomoći u izvršenju zakonite i ovlašćene vladine funkcije.

Član 2

- OGRANIČENJA DEJSTVA SPORAZUMA

Ovaj Sporazum se neće primjenjivati na tajne podatke u okviru uslova drugog sporazuma ili aranžmana između Strana ili agencija, obezbjeđujući stoga zaštitu pojedinih djelova ili kategorija tajnih podataka razmijenjenih između Strana ili agencija, osim u mjeri u kojoj se drugim sporazumom ili aranžmanom uslovi ovog Sporazuma izričito učine primjenljivim. Ovaj Sporazum se takođe neće primjenjivati na razmjenu tajnih podataka, kako je definisano u U.S Atomic Energy Act iz 1954, izmijenjen i dopunjen (the AEA), ili tajnih podataka koji više ne spadaju u tu kategoriju u skladu sa AEA ali se od strane Sjedinjenih Država još uvijek smatraju vojnim podacima.

Član 3

- POSVEĆENOST ZAŠTITI TAJNIH PODATAKA

1. Svaka Strana će štititi tajne podatke druge Strane u skladu sa uslovima utvrđenim ovdje.
2. Tajni podaci će biti zaštićeni od Strane primaoca na način koji je najmanje ekvivalentan zaštiti koja je obezbijeđena tajnim podacima Strane pošiljaoca.
3. Svaka Strana će, bez odlaganja, obavijestiti drugu stranu o svim izmjenama njenih zakona i propisa koji mogu uticati na zaštitu tajnih podataka u okviru ovog Sporazuma. Obaveze koje proističu iz ovog Sporazuma neće biti pod uticajem takvih izmjena nacionalnih propisa. U takvim slučajevima, Strane će se konsultovati o mogućim izmjenama i dopunama ovog Sporazuma ili drugim mjerama koje mogu biti prikladne u cilju održavanja zaštite tajnih podataka razmijenjenih u okviru ovog Sporazuma.

Član 4

- NACIONALNI BEZBJEDNOSNI ORGANI

1. Strane će obavijestiti jedna drugu o Nacionalnim bezbjednosnim organima odgovornim za implementaciju ovog Sporazuma i svim naknadnim izmjenama koji se tiču tih organa.
2. U svrhu ovog Sporazuma, Nacionalni bezbjednosni organi su:

   a. Za Crnu Goru: Direktor, Direkcija za zaštitu tajnih podataka, Crna Gora

   b. Za Sjedinjene Države: Direktor, Međunarodni bezbjednosni programi, Služba bezbjednosnih odbrambenih tehnologija, Kancelarija podsekretara za odbrambenu politiku, Ministarstvo odbrane Sjedinjenih Država
3. Strane mogu zaključiti dodatne aranžmane za implementaciju ovog Sporazuma kojima se mogu zahtijevati dodatne tehničke bezbjednosne mjere za zaštitu tajnih podataka proslijeđenih Strani primaocu putem stranih vojnih prodajnih ili kooperativnih programa za zajedničku proizvodnju i razvoj odbrambenih proizvoda ili usluga. Takvi aranžmani za implementaciju mogu obuhvatati Specijalne bezbjednosne sporazume ili Industrijske bezbjednosne sporazume.

Član 5

- OZNAČAVANJE TAJNIH PODATAKA

1. Tajni podaci će biti označeni, i pečatirani ili obilježeni gdje je to moguće, od Strane pošiljaoca jednim od sljedećih nacionalnih stepena tajnosti. U cilju obezbjeđivanja podjednake zaštite, Strane su se složile da su sljedeći stepeni tajnosti ekvivalentni:

CRNA GORA	UNITED STATES
STROGO TAJNO	TOP SECRET
TAJNO	SECRET
POVJERLJIVO	CONFIDENTIAL

INTERNO (RESTRICTED)	No equivalent

2. Tokom implementacije ovog Sporazuma, ukoliko Crna Gora ustupi tajne podatke stepena tajnosti "INTERNO", Sjedinjene Države će sa njima postupati u skladu sa Dodatkom ovog Sporazuma.
3. Tajni podaci će biti označeni, i pečatirani ili obilježeni gdje je to moguće, imenom Strane pošiljaoca.

Član 6

- ODGOVORNOST ZA TAJNE PODATKE

Strana primalac će biti odgovorna za zaštitu svih tajnih podataka Strane pošiljaoca na način koji će obezbijediti najmanje podjednaku zaštitu koja je tajnim podacima obezbijeđena od Strane pošiljaoca, dok su tajni podaci pod njenom kontrolom. Tokom prenosa, Strana pošiljalac će biti odgovorna za sve tajne podatke sve dok se formalno ne dostave Strani primaocu.

Član 7

- ZAŠTITA TAJNIH PODATAKA

1. Ni jedno lice neće imati pravo pristupa tajnim podacima samo na osnovu čina, radnog mjesta, imenovanja, ili dozvole za pristup tajnim podacima. Pristup takvim podacima odobriće se samo licima u skladu sa principom "potrebno je da zna" i koja imaju izdatu neophodnu dozvolu za pristup tajnim podacima u skladu sa predviđenim standardima Strane primaoca.
2. Ukoliko nije drugačije propisano ovim Sporazumom, Strana primalac neće ustupiti tajne podatke Strane pošiljaoca trećoj strani, uključujući Vladu treće strane, lice, kompaniju, instituciju, organizaciju, ili drugog subjekta, bez prethodne pisane saglasnosti Strane pošiljaoca.
3. Strana primalac neće koristiti ili dozvoliti korišćenje tajnih podataka Strane pošiljaoca u bilo koju drugu svrhu osim u svrhu za koju su ustupljeni bez prethodne pisane saglasnosti Strane pošiljaoca.
4. Strana primalac će poštovati privatna prava koja se odnose na tajne podatke Strane pošiljaoca, uključujući i prava patenata, autorska prava, poslovne tajne i neće ustupati, koristiti, razmjenjivati ili otkrivati takve tajne podatke na način koji je u suprotnosti sa tim pravima bez prethodnog pisanog odobrenja vlasnika tih prava.
5. Strana primalac će obezbijediti da svaki objekat ili ustanova u kojima se rukuje tajnim podacima koje uključuje ovaj Sporazum, ažurira spisak lica u objektu ili ustanovi koja su ovlašćena da pristupaju takvim podacima.
6. Svaka strana će razviti odgovornost i procedure kontrole za upravljanje ustupanjem i pristupom tajnim podacima.
7. Svaka strana će poštovati bilo koja ili sva ograničenja u pogledu korišćenja, otkrivanja, ustupanja i pristupa tajnim podacima koje može odrediti Strana pošiljalac kada dođe do otkrivanja takvih tajnih podataka. Ukoliko Strana nije u mogućnosti da postupi u skladu sa određenim ograničenjima, ta Strana će se bez odlaganja konsultovati sa drugom Stranom i preduzeće sve zakonite mjere kako bi spriječila ili umanjila posljedice takvog korišćenja, otkrivanja, ustupanja ili pristupa.

Član 8

- DOZVOLE ZA PRISTUP TAJNIM PODACIMA FIZIČKIM LICIMA

1. Strane će obezbijediti da se svim licima kojima je radi obavljanja svojih službenih dužnosti potreban pristup ili čije dužnosti i funkcije mogu pružati pristup tajnim podacima u skladu sa ovim Sporazumom, izda odgovarajuća dozvola za pristup tajnim podacima fizičkim licima prije odobravanja pristupa takvim podacima.
2. Strana koja izdaje dozvolu za pristup tajnim podacima fizičkom licu će sprovesti odgovarajuću bezbjednosnu provjeru sa dovoljno detalja da utvrdi podobnost lica za pristup tajnim podacima. Odluka o izdavanju dozvole biće donijeta u skladu sa nacionalnim zakonima i propisima Strane koja izdaje dozvolu.
3. Prije nego zvaničnik ili predstavnik jedne Strane ustupi tajne podatke zvaničniku ili predstavniku druge Strane, Strana primalac će obezbijediti Strani pošiljaocu uvjerenje da zvaničnik ili predstavnik ima dozvolu za pristup tajnim podacima neophodnog stepena tajnosti i "potrebu da zna" kao i da će tajni podaci biti zaštićeni od Strane primaoca u skladu sa ovim Sporazumom.

Član 9

- USTUPANJE TAJNIH PODATAKA UGOVARAČIMA

1. Tajne podatke koje je primila, Strana primalac može ustupiti Ugovaraču ili potencijalnom Ugovaraču čije izvršavanje obaveza zahtijeva pristup takvim podacima uz prethodnu pisanu saglasnost Strane pošiljaoca. Prije ustupanja bilo kog tajnog podatka Ugovaraču ili potencijalnom Ugovaraču, Strana primalac će:

a. potvrditi da Ugovarač ili potencijalni Ugovarač i njihovi objekti zadovoljavaju uslove za čuvanje podataka u skladu sa uslovima ovog Sporazuma;

b. potvrditi da Ugovarač ili potencijalni Ugovarač i njihovi objekti imaju izdatu dozvolu za pristup tajnim podacima za fizička lica i dozvolu za pristup tajnim podacima za pravna lica, ukoliko je primjenljivo;

c. potvrditi da Ugovarač ili potencijalni Ugovarač imaju procedure koje obezbjeđuju da su sva lica koja imaju pristup podacima informisana o svojim obavezama da čuvaju podatke u skladu sa odgovarajućim zakonima i propisima;

d. sprovoditi periodične bezbjednosne kontrole provjerenih objekata kako bi obezbjedila zaštitu podataka u skladu sa zahtjevima ovog Sporazuma; i

e. potvrditi da Ugovarač ili potencijalni Ugovarač imaju procedure koje obezbjeđuju da je pristup podacima ograničen samo na lica koja imaju "potrebu da znaju".

Član 10

- POVJERLJIVI UGOVORI

1. Kada Strana predloži da zaključi, ili ovlasti Ugovarača u svojoj državi da zaključi povjerljivi ugovor koji je označen stepenom tajnosti POVJERLJIVO/ CONFIDENTIAL ili višim, sa Ugovaračem iz države druge Strane, Strana koja zaključuje ili ovlašćuje Ugovarača da zaključi takav povjerljivi ugovor će zahtijevati potvrdu da je izdata dozvola za pristup tajnim podacima za pravno lice od strane Nacionalnog bezbjednosnog organa druge Strane. Nacionalni bezbjednosni organ Strane koja traži potvrdu će nadzirati i preduzimati sve neophodne korake kako bi se obezbjedilo da sve bezbjednosne aktivnosti Ugovarača budu u skladu sa odgovarajućim zakonima i propisima.
2. Nacionalni bezbjednosni organ Strane koja pregovara o zaključenju povjerljivog ugovora koji će se izvršavati na teritoriji druge Strane, će uključiti u povjerljivi ugovor, zahtjev za ponudu, ili dokument o podugovoru odgovarajuće bezbjednosne klauzule i druge odredbe od značaja, uključujući i troškove za bezbjednost. Ovo uključuje i odredbe kojima se zahtijeva od Ugovarača da uključe odgovarajuće bezbjednosne klauzule u svoje podugovore.

Član 11

- ODGOVORNOST ZA OBJEKTE

Svaka Strana će biti odgovorna za bezbjednost svih državnih i privatnih objekata i ustanova gdje se čuvaju tajni podaci druge Strane i obezbijediće da svi takvi objekti i ustanove imaju stručno i odgovarajuće bezbjednosno provjereno osoblje imenovano sa odgovornostima i ovlašćenjima za kontrolu i zaštitu takvih podataka.

Član 12

- ČUVANJE TAJNIH PODATAKA

Tajni podaci razmijenjeni između Strana čuvaće se na način koji obezbjeđuje pristup isključivo licima koja su ovlašćena za pristup.

Član 13

- PRENOS

1. Tajni podaci između Strana će se prenositi vladinim kanalima ili drugim kanalima prethodno međusobno odobrenim u pisanoj formi.
2. Minimum uslova za bezbjednost tajnih podataka prilikom prenosa će biti sljedeći:

a. Dokumenti ili drugi mediji:

(1) Dokumenti ili drugi mediji koji sadrže tajne podatke prenosiće se u dvije zapečaćene koverte. Na unutrašnjoj koverti će biti samo oznaka stepena tajnosti dokumenata ili drugog medija kao i adresa primaoca kome su namijenjeni. Na spoljašnjoj koverti će biti samo adresa primaoca, adresa pošiljaoca i kontrolni broj dokumenta, ukoliko je primjenljivo.

(2) Na spoljnoj koverti neće biti oznaka stepena tajnosti dokumenata ili drugih medija koji su u njoj. Zapečaćeni dupli koverat će se prenositi u skladu sa propisanim procedurama Strana.

(3) Potvrde o prijemu će biti pripremljene od strane primaoca za pakovanja koja sadrže dokumenta ili druge medije sa tajnim podacima koji se razmjenjuju između Strana, i te potvrde će biti potpisane od strane krajnjeg primaoca i vraćene pošiljaocu.

b. Materijal:

(1) Materijal, uključujući i opremu, koji sadrži tajne podatke prenosiće se zapečaćenim, zaštitnim vozilima, ili će u suprotnom biti bezbjedno spakovani ili zaštićeni na način da se ne može identifikovati njihov oblik, veličina, sadržaj, i biće pod stalnim nadzorom kako bi se spriječio pristup neovlašćenim licima.

(2) Materijal, uključujući i opremu, koji sadrži tajne podatke koji se moraju privremeno čuvati do slanja biće smješteni u zaštićene zone za skladištenje. Te zone će imati opremu za zaštitu od neovlašćenog ulaska ili stražare sa odgovarajućom dozvolom za pristup tajnim podacima koji će u kontinuitetu vršiti kontrolu ovih zona. Samo ovlašćena lica sa odgovarajućom dozvolom za pristup tajnim podacima će imati pristup tim zaštićenim zonama.

(3) Potvrde o prijemu se izdaju uvijek kada materijal koji sadrži tajne podatke, uključujući opremu, mijenja prenosioce tokom tranzita, i potvrda o prijemu takvog materijala biće potpisana od strane krajnjeg primaoca i vraćena pošiljaocu.

c. Elektronski prenos:

(1) Tajni podaci označeni stepenom tajnosti POVJERLJIVO/CONFIDENTIAL ili višim koji se prenose elektronskim putem prenosiće se bezbjednosnim sredstvima koja su odobrena od strane oba Nacionalna bezbjednosna organa Strana.

Član 14

- POSJETE OBJEKTIMA I STRUKTURAMA STRANA

1. Posjete predstavnika jedne strane objektima i strukturama druge Strane koje zahtijevaju pristup tajnim podacima, ili posjete za koje se zahtijeva dozvola za pristup tajnim podacima da bi se omogućio pristup, biće ograničene na one koje su neophodne za službene potrebe. Ovlašćenja će biti data jedino predstavnicima koji imaju važeću dozvolu za pristup tajnim podacima fizičkom licu.
2. Ovlašćenja za posjete takvih objekata i struktura izdaće Strana na čijoj teritoriji se nalaze objekti i strukture koje treba posjetiti. Strana koja se posjećuje, ili njeni zvaničnici određeni za to, biće odgovorna za upoznavanje objekata ili struktura sa predloženom posjetom, i obimom i najvišim stepenom tajnosti podataka sa kojima mogu biti upoznati posjetioci.
3. Zahtjevi za posjetu predstavnika Strana podnosiće se preko Ambasade Sjedinjenih Država u Podgorici, u slučaju posjetioca iz Sjedinjenih Država, i putem Ambasade Crne Gore u Vašingtonu, u slučaju posjetioca iz Crne Gore.

Član 15

- BEZBJEDNOSNE POSJETE

Implementacija bezbjednosnih zahtijeva utvrđenih ovim Sporazumom može biti potvrđena recipročnim posjetama od strane lica koja se bave poslovima zaštite i bezbjednosti Strana. Predstavnicima koji se bave poslovima zaštite i bezbjednosti svake Strane, nakon prethodno obavljenih konsultacija, biće odobrena posjeta drugoj Strani kako bi vidjeli i razmotrili implementaciju procedura druge Strane u cilju postizanja razumne uporedivosti bezbjednosnih sistema. Strana domaćin će tokom posjete pružiti pomoć predstavnicima koji se bave poslovima zaštite i bezbjednosti u cilju utvđjivanja da li su tajni podaci primljeni od druge Strane adekvatno zaštićeni.

Član 16

- BEZBJEDNOSNI STANDARDI

Na zahtjev, svaka Strana će obezbijediti drugoj Strani informacije o njenim bezbjednosnim standardima, praksama i procedurama zaštite tajnih podataka.

Član 17

- UMNOŽAVANJE TAJNIH PODATAKA

Prilikom umnožavanja tajnih podataka, sve originalne oznake stepena tajnosti kojima je podatak označen, će biti umnožene, pečati- rane ili označene na svakom umnoženom primjerku podatka. Takvi umnoženi podaci će biti predmet iste kontrole kao i original podatka. Broj umnoženih primjeraka biće ograničen na minimalan broj primjeraka potreban za službenu upotrebu.

Član 18

- UNIŠTAVANJE TAJNIH PODATAKA

1. Dokumenti i drugi mediji koji sadrže tajne podatke biće uništeni paljenjem, sjeckanjem, rezanjem ili drugim sredstvima koja onemogućavaju rekonstrukciju tajnih podataka koje sadrže.

2. Materijal, uključujući i opremu, koji sadrži tajne podatke će se uništiti na način da podatak više neće biti prepoznatljiv u cilju sprječavanja rekonstrukcije tajnog podatka u cjelosti ili nekog njegovog dijela.

Član 19

- SMANJIVANJE ILI UKIDANJE STEPENA TAJNOSTI

1. Strane su saglasne da treba smanjiti stepen tajnosti tajnog podatka odmah po prestanku potrebe da podatak ima prethodni viši stepen tajnosti ili da treba ukinuti stepen tajnosti odmah kada taj podatak ne zahtijeva više zaštitu od neovlašćenog otkrivanja.
2. Strana pošiljalac ima potpunu diskreciju u vezi sa smanjivanjem ili ukidanjem stepena tajnosti svojih tajnih podataka. Strana primalac neće smanjivati ili ukidati stepen tajnosti tajnih podataka primljenih od druge Strane, bez obzira na postojeće instrukcije u vezi sa ukidanjem stepena tajnosti dokumenta, bez prethodne pisane saglasnosti Strane pošiljaoca.

Član 20

- GUBITAK I POVREDA BEZBJEDNOSTI

Strana primalac će bez odlaganja obavijestiti Stranu pošiljaoca kada otkrije gubitke ili povrede bezbjednosti, kao i o mogućim gubicima ili povredama bezbjednosti tajnih podataka Strane pošiljaoca. U slučaju stvarnih ili mogućih gubitaka ili povreda bezbjednosti takvih podataka, Strana primalac će bez odlaganja pokrenuti istragu u cilju utvrđivanja okolnosti pod kojima je došlo do stvarnog ili mogućeg gubitka ili povrede bezbjednosti. Rezultate istrage i mjere koje su preduzete u cilju sprječavanja ponavljanja biće obezbijeđene Strani pošiljaocu.

Član 21

- SPOROVI

Neslaganja između Strana koja nastaju iz ovog Sporazuma ili su u vezi sa njim rješavaće se isključivo putem konsultacija između Strana i neće biti predati na rješavanje nacionalnom sudu, međunarodnom sudu, ili bilo kom drugom licu ili subjektu.

Član 22

- TROŠKOVI

Svaka strana će snositi svoje troškove nastale implementacijom ovog Sporazuma. Sve obaveze Strana u skladu sa ovim Sporazumom će zavisiti od raspoloživosti finansijskih sredstava.

Član 23

- ZAVRŠNE ODREDBE

1. Ovaj Sporazum stupa na snagu datumom poslednjeg potpisa Strana.
2. Svaka Strana može otkazati ovaj Sporazum obavještavajući pisanim putem drugu Stranu putem diplomatskih kanala devedeset dana prije namjere da otkaže Sporazum.
3. Bez obzira na otkazivanje ovog Sporazuma, svi tajni podaci razmijenjeni ili na drugi način ustupljeni u skladu sa ovim Sporazumom nastaviće da se štite u skladu sa postojećim odredbama.

Potvrđujući ovo, dolje potpisani, propisno ovlašćeni od strane svojih Vlada, potpisali su ovaj Sporazum.

Sačinjeno u Vašingtonu, dana 27. februara 2018. godine, u dva primjerka na crnogorskom i engleskom jeziku, pri čemu su oba teksta jednako vjerodostojna. U slučaju razlika u tumačenju, mjerodavan je tekst na engleskom jeziku.

Za Vladu Crne Gore

Predrag Bošković, s.r.

Ministar odbrane

Za Vladu Sjedinjenih Američkih Država

James N. Mattis, s.r.

Ministar odbrane

DODATAK

PROCEDURE ZA POSTUPANJE SA PODACIMA OZNAČENIM STEPENOM TAJNOSTI "INTERNO" U SJEDINJENIM AMERIČKIM DRŽAVAMA

1. Po prijemu, tajni podaci Crne Gore koji su ustupljeni Sjedinjenim Državama i označeni stepenom tajnosti "INTERNO", Sjedinjene Države će štititi u skladu sa sljedećim procedurama.

2. Podaci označeni stepenom tajnosti "INTERNO" čuvaće se u zaključanim kasama ili zaštićenim zonama koje će onemogućiti pristup neovlašćenim licima.
3. Podaci označeni stepenom "INTERNO" neće biti otkriveni neovlašćenim licima ili organima bez prethodne pisane saglasnosti Vlade Crne Gore osim u slučajevima propisanim zakonom Sjedinjenih Država, uključujući i Zakon o slobodi informisanja.
4. Podaci označeni stepenom "INTERNO", gdje je primjenljivo, će se čuvati, obrađivati i prenositi elektronskim putem posredstvom Vladinih ili sertifikovanih sistema Ugovarača. Posebno, prije početka korišćenja svakog sistema za čuvanje, obrađivanje ili prenošenje elektronskim putem tajnih podataka označenih stepenom "INTERNO", sistem mora da dobije bezbjednosno odobrenje, odnosno akreditaciju. Akreditacija je formalna izjava odgovarajućeg tijela za akreditaciju kojom se potvrđuje da upotreba sistema zadovoljava odgovarajuće bezbjednosne zahtjeve i ne predstavlja neprihvatljiv rizik. Standardne bezbjednosne operativne procedure su tehničke procedure za implementaciju bezbjednosnih politika i zahtijeva jedinstvenih za određeni objekat za zaštitu automatizovanog informacionog sistema za obradu tajnih podataka. Za nezavisne automatizovane informacione sisteme kao što su stoni ili prenosivi računari (desktop/laptop kompjuteri) koji se koriste u ustanovama Vlade Sjedinjenih Država, registracioni dokument za određeni sistem zajedno sa Standardnim bezbjednosno operativnim procedurama imaće ulogu potrebne akreditacije. Za ugovarače, uputstvo za upotrebu komunikaciono informacionih sistema biće sadržano u klauzuli o zahtjevima za uslove ograničenog pristupa u ugovoru.
5. Podaci označeni stepenom tajnosti "INTERNO" prenosiće se poštom prve klase unutar Sjedinjenih Država, u jednoj zapečaćenoj koverti. Prenos izvan Sjedinjenih Država vršiće se u dvije zapečaćene koverte, pri čemu je unutrašnji koverat označen oznakom "CRNA GORA INTERNO". Prenosi izvan Sjedinjenih Država vršiće se sredstvima koja se mogu pratiti, kao što su komercijalni kuriri ili druga sredstva o kojima se postigne pisani dogovor između Strana.
6. Podaci Sjedinjenih Država koji sadrže podatke "CRNA GORA INTERNO" nosiće na omotu i prvoj strani oznaku "CRNA GORA INTERNO". Djelovi dokumenata koji sadrže podatke označene "CRNA GORA INTERNO" takođe će biti označeni istom oznakom.
7. Podaci označeni stepenom tajnosti "INTERNO" mogu se prenositi ili se podacima može pristupati putem javnih mreža kao interneta koristeći Vladine ili komercijalne uređaje za kripto-zaštitu koje su Strane zajednički odobrile. Prenosi putem telefonskih razgovora, video-konferencija ili faksimila koji sadrže podatke sa oznakom "INTERNO" mogu se vršiti ukoliko sistem kripto-zaštite nije dostupan i predmet je odobrenja Nacionalnog bezbjednosnog organa Strane pošiljaoca.
8. Dozvola za pristup tajnim podacima pravnom licu ne zahtijeva se od Ugovarača koji izvršava ugovore koji zahtijevaju samo prijem ili nastanak tajnih podataka označenih stepenom tajnosti "INTERNO".
9. Pristup tajnim podacima označenim stepenom tajnosti "INTERNO" biće odobren samo onim licima koji imaju potrebu da znaju. Dozvola za pristup tajnim podacima fizičkom licu se ne zahtijeva za pristup tajnim podacima označenim stepenom tajnosti "INTERNO".

AGREEMENT BETWEEN THE GOVERNMENT OF MONTENEGRO AND THE GOVERNMENT OF THE UNITED STATES OF AMERICA CONCERNING SECURITY MEASURES FOR THE PROTECTION OF CLASSIFIED INFORMATION

PREAMBLE

The Government of Montenegro ("Montenegro") and the Government of the United States of America (the "United States") (each a "Party," and collectively the "Parties"),

Considering that the Parties cooperate in matters including, but not limited to, foreign affairs, defense, security, law enforcement, science, industry, and technology, and

Having a mutual interest in the protection of Classified Information exchanged in confidence between the Parties,

Have agreed as follows:

ARTICLE 1 – DEFINITIONS

For the purpose of this Agreement:

1. Classified Information: Information provided by one Party to the other Party that is designated as classified by the releasing Party for national security purposes and therefore requires protection against unauthorized disclosure. The information may be in oral, visual, electronic, or documentary form, or in the form of material, including equipment or technology.

2. Classified Contract: A contract that requires, or will require, access to, or production of, Classified Information by a Contractor or by its employees in the performance of the contract.

3. Contractor: An individual or a legal entity, possessing the legal capacity to conclude contracts, who is a party to a Classified Contract.

4. Facility Security Clearance: A certification provided by the National Security Authority of a Party, as designated in Article 4, for a Contractor facility under the Party's jurisdiction that indicates the facility is cleared to a specified level and also has suitable security safeguards in place at a specified level to safeguard Classified Information. Such a certification shall signify that Classified Information at the POVJERLJIVO / CONFIDENTIAL level or above shall be protected by the Contractor for which the Facility Security Clearance (FSC) is provided in accordance with the provisions of this Agreement and that compliance shall be monitored and enforced by the relevant National Security Authority. An FSC is not required for a Contractor to undertake contracts that only require the receipt or production of Classified Information at the INTERNO (RESTRICTED) level.

5. Personnel Security Clearance (PSC):

a. A determination by the National Security Authority of a Party, as designated in Article 4, that an individual who is employed by a government agency of that Party or a Contractor under the jurisdiction of that Party is authorized to access Classified Information up to a specified level.

b. A determination by the National Security Authority of a Party, as designated in Article 4, that an individual who is a citizen of one Party but is to be employed by the other Party or by one of the other Party's Contractors is authorized access to Classified Information up to a specified level.

6. Need to Know: A determination made by an authorized holder of Classified Information that a prospective recipient of Classified Information requires access to specific Classified Information in order to perform or assist in a lawful and authorized governmental function.

ARTICLE 2 – LIMITATIONS ON SCOPE OF THE AGREEMENT

This Agreement shall not apply to Classified Information within the scope of the terms of another agreement or arrangement between the Parties or agencies thereof providing for the protection of a particular item or category of Classified Information exchanged between the Parties or agencies thereof, except to the extent that such other agreement or arrangement expressly makes this Agreement's terms applicable. This Agreement also shall not apply to the exchange of Restricted Data, as defined in the U.S. Atomic Energy Act of 1954, as amended (the "AEA"), or to Formerly Restricted Data, which is data removed from the Restricted Data category in accordance with the AEA but still considered to be defense information by the United States.

ARTICLE 3 – COMMITMENT TO THE PROTECTION OF CLASSIFIED INFORMATION

1. Each Party shall protect Classified Information of the other Party according to the terms set forth herein.

2. Classified Information shall be protected by the recipient Party in a manner that is at least equivalent to the protection afforded to Classified Information by the releasing Party.

3. Each Party shall promptly notify the other of any changes to its laws and regulations that would affect the protection of Classified Information under this Agreement. The obligations in this Agreement shall not be affected by such changes in domestic law. In such cases, the Parties shall consult regarding possible amendments to this Agreement or other measures that may be appropriate to maintain protection of Classified Information exchanged under this Agreement.

ARTICLE 4 – NATIONAL SECURITY AUTHORITIES

1. The Parties shall inform each other of the National Security Authorities responsible for implementation of this Agreement and any subsequent changes to these Authorities.

2. For the purpose of this Agreement, the National Security Authorities shall be:

a. For Montenegro: Director, National Security Authority, Montenegro

b. For the United States: Director, International Security Programs, Defense Technology Security Administration, Office of the Under Secretary of Defense for Policy, Department of Defense of the United States of America

3. The Parties may conclude supplemental implementing arrangements to this Agreement where additional technical security measures may be required to protect Classified Information transferred to the recipient Party through foreign military sales or cooperative programs for co-production or co-development of defense articles or services. Such implementing arrangements may include Special Security Agreements or Industrial Security Agreements.

ARTICLE 5 – DESIGNATION OF CLASSIFIED INFORMATION

1. Classified Information shall be designated, and stamped or marked where possible, by the releasing Party as classified at one of the following national security classification levels. For purposes of ensuring equivalent treatment, the Parties agree that the following security classification levels are equivalent:

MONTENEGRO	**UNITED STATES**
STROGO TAJNO	TOP SECRET
TAJNO	SECRET
POVJERLJIVO	CONFIDENTIAL
INTERNO	No equivalent
(RESTRICTED)	

2. During the implementation of this Agreement, if Montenegro provides Classified Information designated as "INTERNO," the United States shall handle it in accordance with the Appendix to this Agreement.

3. Classified Information shall be designated, and stamped or marked where possible, with the name of the releasing Party.

ARTICLE 6 – RESPONSIBILITY FOR CLASSIFIED INFORMATION

The recipient Party shall be responsible for the protection of all Classified Information of the releasing Party in a manner that is at least equivalent to the protection afforded to Classified Information by the releasing Party while the Classified Information is under its control. While in transit, the releasing Party shall be responsible for all Classified Information until custody of the Classified Information is formally transferred to the recipient Party.

ARTICLE 7 – PROTECTION OF CLASSIFIED INFORMATION

1. No individual shall be entitled to have access to Classified Information solely by virtue of rank, position, appointment, or PSC. Access to such information shall be granted only to individuals who have a Need to Know and who have been granted the requisite PSC in accordance with the prescribed standards of the recipient Party.

2. Except as otherwise provided in this Agreement, the recipient Party shall not release Classified Information of the releasing Party to any third party, including any third-party government, individual, firm, institution, organization, or other entity, without the prior written consent of the releasing Party.

3. The recipient Party shall not use or permit the use of Classified Information of the releasing Party for any other purpose than that for which it was provided without the prior written consent of the releasing Party.

4. The recipient Party shall respect any private rights that are associated with Classified Information of the releasing Party, including those rights with respect to patents, copyrights, or trade secrets, and shall not release, use, exchange, or disclose such Classified Information in a manner inconsistent with those rights without the prior written authorization of the owner of those rights.

5. The recipient Party shall ensure that each facility or establishment that handles Classified Information covered by this Agreement maintains a list of individuals at the facility or establishment who are authorized to have access to such information.

6. Each Party shall develop accountability and control procedures to manage the dissemination of, and access to, Classified Information.

7. Each Party shall comply with any and all limitations on use, disclosure, release, and access to Classified Information as may be specified by the releasing Party when it discloses such Classified Information. If a Party is unable to comply with the specified limitations, that Party shall immediately consult with the other Party and shall undertake all lawful measures to prevent or minimize any such use, disclosure, release, or access.

ARTICLE 8 – PERSONNEL SECURITY CLEARANCES

1. The Parties shall ensure that all individuals who in the conduct of their official duties require access or whose duties or functions may afford access to Classified Information pursuant to this Agreement receive an appropriate PSC before they are granted access to such information.

2. The Party granting the PSC shall conduct an appropriate investigation in sufficient detail to determine an individual's suitability for access to Classified Information. The determination to grant a PSC will be made in accordance with the national laws and regulations of the granting Party.

3. Before an official or representative of one Party releases Classified Information to an official or representative of the other Party, the recipient Party shall provide to the releasing Party an assurance that the official or representative has the necessary PSC level and a Need to Know and that the Classified Information will be protected by the recipient Party in accordance with this Agreement.

ARTICLE 9 – RELEASE OF CLASSIFIED INFORMATION TO CONTRACTORS

1. Classified Information received by a recipient Party may be provided by the recipient Party to a Contractor or prospective Contractor whose duties require access to such information with the prior written consent of the releasing Party. Prior to releasing any Classified Information to a Contractor or prospective Contractor, the recipient Party shall:

a. Confirm that such Contractor or prospective Contractor and the Contractor's facility have the capability to safeguard the information in accordance with the terms of this Agreement;

b. Confirm that such Contractor or prospective Contractor and the Contractor's facility have been granted appropriate PSCs and FSCs, as applicable;

c. Confirm that the Contractor or prospective Contractor has procedures in place to ensure that all individuals having access to the information are informed of their responsibilities to protect the information in accordance with applicable laws and regulations;

d. Carry out periodic security inspections of cleared facilities to ensure that the information is protected as required by this Agreement; and

e. Confirm that the Contractor or prospective Contractor has procedures in place to ensure that access to the information is limited to those individuals who have a Need to Know.

ARTICLE 10 – CLASSIFIED CONTRACTS

1. When a Party proposes to place, or authorizes a Contractor in its country to place, a Classified Contract that is classified at the POVJERLJIVO / CONFIDENTIAL level or above, with a Contractor in the country of the other Party, the Party that is to place or authorize the Contractor to place such Classified Contract shall request an assurance that an FSC has been issued from the National Security Authority of the other Party. The National Security Authority of the requested Party shall monitor and take all appropriate steps to ensure the security conduct by the Contractor will be in accordance with applicable laws and regulations.

2. The National Security Authority of a Party negotiating a Classified Contract to be performed in the country of the other Party shall incorporate in the Classified Contract, request for proposal, or subcontract document appropriate security clauses and other relevant provisions, including costs for security. This includes provisions requiring any Contractors to include appropriate security clauses in their subcontract documents.

ARTICLE 11 – RESPONSIBILITY FOR FACILITIES

Each Party shall be responsible for the security of all government and private facilities and establishments where it stores Classified Information of the other Party and shall ensure that such facilities or establishments have qualified and appropriately cleared individuals appointed with the responsibility and authority for the control and protection of such information.

ARTICLE 12 – STORAGE OF CLASSIFIED INFORMATION

Classified Information exchanged between the Parties shall be stored in a manner that ensures access only by those individuals who have been authorized access.

ARTICLE 13 – TRANSMISSION

1. Classified Information shall be transmitted between the Parties through government-to-government channels or other channels mutually approved in advance in writing.

2. The minimum requirements for the security of Classified Information during transmission shall be as follows:

a. Documents or other media:

(1) Documents or other media containing Classified Information shall be transmitted in double, sealed envelopes. The inner envelope shall indicate only the classification of the documents or other media and the organizational address of the intended recipient. The outer envelope shall indicate the organizational address of the intended recipient, the organizational address of the sender, and the document control number, if applicable.

(2) No indication of the classification of the enclosed documents or other media shall be made on the outer envelope. The double sealed envelope shall be transmitted according to the prescribed procedures of the Parties.

(3) Receipts shall be prepared by the recipient for packages containing documents or other media containing Classified Information that are transmitted between the Parties, and such receipts shall be signed by the final recipient and returned to the sender.

b. Material:

(1) Material, including equipment, that contains Classified Information shall be transported in sealed, covered vehicles, or shall otherwise be securely packaged or protected in order to prevent identification of its shape, size, or contents, and kept under continuous control to prevent access by unauthorized persons.

(2) Material, including equipment that contains Classified Information that must be stored temporarily awaiting shipment shall be placed in protected storage areas. Such areas shall be protected by intrusion detection equipment or guards with requisite PSCs who shall maintain continuous surveillance of those areas. Only authorized personnel with the requisite PSC shall have access to the protected storage areas.

(3) Receipts shall be obtained whenever material that contains Classified Information, including equipment, changes hands during transit, and a receipt for such material shall be signed by the final recipient and returned to the sender.

c. Electronic transmissions:

(1) Classified Information that is classified at the CONFIDENTIAL / POVJERLJIVO level or above that is to be transferred electronically shall be transmitted using secure means that have been approved by each Party's National Security Authority.

ARTICLE 14 – VISITS TO FACILITIES AND ESTABLISHMENTS OF THE PARTIES

1. Visits by representatives of one Party to facilities and establishments of the other Party that require access to Classified Information, or visits for which a PSC is required to permit access, shall be limited to those necessary for official purposes. Authorization shall only be granted to representatives who possess a valid PSC.

2. Authorization to visit such facilities and establishments shall be granted only by the Party in whose territory the facility or establishment to be visited is located. The visited Party, or its designated officials, shall be responsible for advising the facility or establishment of the proposed visit, and the scope and highest level of Classified Information that may be furnished to the visitor.

3. Requests for visits by representatives of the Parties shall be submitted by the Embassy of the United States in Podgorica in the case of U.S. visitors, and by the Embassy of Montenegro in Washington, D.C., in the case of Montenegrin visitors.

ARTICLE 15 – SECURITY VISITS

Implementation of security requirements set out in this Agreement may be verified through reciprocal visits by security personnel of the Parties. The security representatives of each Party, after prior consultation, shall be permitted to visit the other Party to discuss and observe the implementing procedures of the other Party in the interest of achieving reasonable comparability of security systems. The

host Party shall assist the visiting security representatives in determining whether Classified Information received from the other Party is being adequately protected.

ARTICLE 16 – SECURITY STANDARDS

On request, each Party shall provide the other Party with information about its security standards, practices, and procedures for safeguarding of Classified Information.

ARTICLE 17 – REPRODUCTION OF CLASSIFIED INFORMATION

When Classified Information is reproduced, all of the original security markings thereon shall also be reproduced, stamped, or marked on each reproduction of such information. Such reproductions shall be subject to the same controls as the original information. The number of reproductions shall be limited to the minimum number required for official purposes.

ARTICLE 18 – DESTRUCTION OF CLASSIFIED INFORMATION

1. Documents and other media containing Classified Information shall be destroyed by burning, shredding, pulping, or other means that prevent reconstruction of the Classified Information contained therein.

2. Material, including equipment, containing Classified Information shall be destroyed through means that render it no longer recognizable so as to preclude reconstruction of the Classified Information in whole or in part.

ARTICLE 19 – DOWNGRADING AND DECLASSIFICATION

1. The Parties agree that Classified Information should be downgraded in classification as soon as the information ceases to require that higher degree of protection or should be declassified as soon as the information no longer requires protection against unauthorized disclosure.

2. The releasing Party has complete discretion concerning downgrading or declassification of its Classified Information. The recipient Party shall not downgrade the security classification or declassify Classified Information received from the releasing Party, notwithstanding any apparent declassification instructions on the document, without the prior written consent of the releasing Party.

ARTICLE 20 – LOSS OR COMPROMISE

The recipient Party shall inform the releasing Party immediately upon discovery of all losses or compromises, as well as possible losses or compromises, of Classified Information of the releasing Party. In the event of an actual or possible loss or compromise of such information, the recipient Party shall initiate an investigation immediately to determine the circumstances of the actual or possible loss or compromise. The results of the investigation and information regarding measures taken to prevent recurrence shall be provided to the releasing Party.

ARTICLE 21 – DISPUTES

Disagreements between the Parties arising under or relating to this Agreement shall be settled solely through consultations between the Parties and shall not be referred to a national court, an international tribunal, or any other person or entity for settlement.

ARTICLE 22 – COSTS

Each Party shall be responsible for bearing its own costs incurred in implementing this Agreement. All obligations of the Parties under this Agreement shall be subject to the availability of funds.

ARTICLE 23 – FINAL PROVISIONS

1. This Agreement shall enter into force upon the date of the last signature by the Parties.

2. Either Party may terminate this Agreement by notifying the other Party in writing through diplomatic channels ninety days in advance of its intention to terminate the Agreement.

3. Notwithstanding the termination of this Agreement, all Classified Information exchanged or otherwise provided pursuant to this Agreement shall continue to be protected in accordance with the provisions set forth herein.

IN WITNESS WHEREOF, the undersigned, being duly authorized thereto by their respective Governments, have signed this Agreement.

DONE in duplicate at Washington, D.C., this 27th day of February, 2018, in the Montenegrin and English languages, both texts being equally authentic. In case of any divergence of interpretation, the English text shall prevail.

FOR THE GOVERNMENT OF
MONTENEGRO:
Predrag Bošković, s.r.
Minister of Defense

FOR THE GOVERNMENT OF
THE UNITED STATES OF AMERICA:
James N. Mattis, s.r.
Secretary of Defense

APPENDIX

PROCEDURES FOR PROTECTING MONTENEGRO INTERNO (RESTRICTED) CLASSIFIED INFORMATION PROVIDED TO THE UNITED STATES

1. Upon receipt, Montenegro Classified Information provided to the United States and designated as "INTERNO" shall be protected by the United States in accordance with the following procedures.

2. Information designated as "INTERNO" shall be stored in locked containers or closed areas that prevent access by unauthorized personnel.

3. "INTERNO" information shall not be disclosed to unauthorized persons or entities without the prior written approval of the Government of Montenegro except as required by U.S. law, including the Freedom of Information Act.

4. "INTERNO" information shall, as applicable, be stored, processed, or transmitted electronically using government- or Contractor-accredited systems. In particular, before any system is used to store, process, or transmit "INTERNO" information, it must receive security approval, known as Accreditation. An Accreditation is a formal statement by the appropriate accrediting authority confirming that the use of a system meets the appropriate security requirements and does not present an unacceptable risk. Security Standard Operating Procedures are technical procedures to implement security policies and requirements unique to a specific facility to protect automated information systems processing Classified Information. For stand-alone automated information systems such as desktop and laptop computers utilized in U.S. Government establishments, the system registration document together with the Security Standard Operating

Procedures shall fulfill the role of the required Accreditation. For Contractors, guidance on the use of communications and information systems shall be incorporated into the Restricted Conditions Requirements Clause in the contract.

5. "INTERNO" information shall be transmitted by first class mail within the United States in one sealed envelope. Transmission outside the United States shall be in double, sealed envelopes, with the inner envelope marked "MONTENEGRO INTERNO." Transmission outside the United States shall be by traceable means such as commercial courier or other means agreed upon by the Parties in writing.

6. U.S. documents that contain "MONTENEGRO INTERNO" information shall bear on the cover and the first page the marking "MONTENEGRO INTERNO." The portion of the documents containing "MONTENEGRO INTERNO" information also shall be identified with the same marking.

7. "INTERNO" information may be transmitted or accessed electronically via a public network like the Internet using government or commercial encryption devices mutually accepted by the Parties. Telephone conversations, video conferencing, or facsimile transmissions containing "INTERNO" information may be conducted if an encryption system is not available and subject to the approval of the releasing Party's National Security Authority.

8. An FSC is not required for a Contractor to undertake contracts that require only the receipt or production of Classified Information at the "INTERNO" level.

9. Access to such "INTERNO" information shall be granted only to those individuals who have a Need to Know. A PSC is not required to access "INTERNO" information.

Član 3

Ova odluka stupa na snagu osmog dana od dana objavljivanja u "Službenom listu Crne Gore-Međunarodni ugovori".

Broj: 07-2477

Podgorica, 4. maj 2018. godine

Vlada Crne Gore

Predsjednik,

Duško Marković, s.r.