**Ostala razmatranja za obrambenu industriju**

Posebni faktori visokog rizika za strana trgovačka društva koja se bave obrambenim proizvodima s podrijetlom iz SAD-a

Prilikom poslovanja s obrambenim proizvodima podrijetlom iz SAD-a vaše će se poduzeće suočiti s jedinstvenim izazovima u vezi sa usklađenošću. Poduzeća moraju razumjeti ograničenja koja se odnose na uključivanje robe podrijetlom iz SAD-a i strani nacionalni pristup kontroliranim proizvodima i tehnologijama podrijetlom iz SAD-a. U nastavku je naveden popis nekih potencijalnih problema s kojima se vaše poduzeće može susresti ako se bavi s obrambenim proizvodima podrijetlom iz SAD-a.

1. Ako strano trgovačko društvo ugradi dio, komponentu, dodatak ili dodatnu opremu koji podliježu nadzoru međunarodnih propisa o trgovini oružja (ITAR), cijeli proizvod podliježe nadzoru u skladu s ITAR-om. Strana trgovačka društva u obrambenom sektoru trebaju biti oprezna kada u svoje gotove proizvode ugrađuju dijelove, komponente, dodatke i dodatnu opremu koja podliježe nadzoru ITAR-a jer na taj način njihovi proizvodi mogu biti podvrgnuti nadležnosti i propisima američkog strateškog nadzora trgovine (poznato kao **pravilo transparentnosti**). Trgovačka društva trebala bi biti upoznata kako će upotreba dijelova koji podliježu nadzoru ITAR-a utjecati na skupinu kontrola za čiju provedbu će postati odgovorna u odnosu na gotove proizvode.
2. Ako su strani državljani zaposleni u američkoj podružnici stranog trgovačkog društva, takvim osobama nije dozvoljen pristup obrambenim proizvodima ili tehničkim podacima koji podliježu nadzoru ITAR-a, osim ako se za to ishodi dozvola ili se primjenjuje izuzeće.
3. Ako strani rukovoditelji stranog trgovačkog društva putuju u podružnicu u SAD-u na sastanke uprave, inspekcije postrojenja i druge potrebe, takvim osobama nije dozvoljen pristup obrambenim proizvodima ili tehničkim podacima koji podliježu nadzoru ITAR-a, osim ako se za to ishodi dozvola ili se primjenjuje izuzeće.
4. Ako američki zaposlenici u podružnici stranog trgovačkog društva u SAD-u putuju u podružnicu u inozemstvo, nije im dopušteno donositi ili raspravljati o obrambenim proizvodima ili tehničkim podacima koji podliježu nadzoru ITAR-a, osim ako za to ne postoji dozvola ili se primjenjuje izuzeće.
5. Ako američki zaposlenici u podružnici strane tvrtke u SAD-u komuniciraju sa zaposlenicima koji su strani državljani u stranom matičnom trgovačkom društvu putem poruka e-pošte, telefonskih poziva, internih dopisa, WebEx sastanaka ili drugih oblika elektroničke komunikacije, američkim zaposlenicima nije dopušteno otkrivati tehničke podatke koji podliježu nadzoru ITAR-a, osim ako se za to ishodi dozvola ili se primjenjuje izuzeće.
6. Ako strano trgovačko društvo proizvede proizvod koji je naveden na Popisu streljiva Sjedinjenih Američkih Država (USML) i ako će se taj proizvod otpremiti u Sjedinjene Američke Države, on postaje proizvod koji podliježe nadzoru ITAR-a i nadležnosti američkog Ministarstva vanjskih poslova.
7. Ako američka podružnica stranog trgovačkog društva u svom računalnom sustavu u SAD-u pohranjuje tehničke podatke ili softvere (poslužitelji, „oblak“, radne stanice sustava, prijenosna računala i drugi uređaji) koji podliježu nadzoru ITAR-a, trgovačko društvo mora američki podatkovni sustav odvojiti „zaštitnim zidom“od računalnih resursa stranog matičnog trgovačkog društva i ostalih stranih podružnica.
8. Stranim trgovačkim društvima nije dozvoljeno registrirati se u Upravi za nadzor trgovine obrambenim materijalima (DDTC) ili podnijeti zahtjev za dozvolu, osim ako osnuju podružnicu u skladu s američkim pravom (neke iznimke se primjenjuju kao u slučaju podnošenja zahtjeva za ovlaštenje za ponovni prijenos u inozemstvo).
9. Sjedinjene Američke Države također primjenjuju posebna pravila na zaposlenike matičnog trgovačkog društva koji imaju dvojno državljanstvo i državljanstvo trećih zemalja. Vaše se poduzeće može odlučiti da želi identificirati osobe s dvojnim državljanstvom i državljanstvom trećih zemalja tijekom postupka zapošljavanja (ovo se može primjenjivati samo u zemljama u kojima se primjenjuje kontrola tzv. „pretpostavljenog“ izvoza).[[1]](#endnote-1)
10. Gore navedena pravila primjenjuju se i kada strano trgovačko društvo kupuje američko trgovačko društvo u sektorima zrakoplovstva, satelita, elektronike, komunikacija, bespilotnih letjelica, pomorstva i drugim obrambenim industrijama.

Razmatranja za IT i računalnu sigurnost

* Ako vaše poduzeće proizvodi tehnologije povezane s oružjem ili provodi istraživanja i razvoj (R&D) koji uključuju tehničke podatke ili informacije koji su povezani s oružjem, preporučuje se da vaše poduzeće **uspostavi sofisticirani informatički i sustav računalne sigurnosti**. Računalni napadi postaju sve sofisticiraniji i sve ih više sponzoriraju države. Zbog toga se **poduzeća koja se bave kontroliranim tehnologijama moraju aktivno i učinkovito obraniti od zlonamjernih softvera, virusa i napada «nultog dana»**.[[2]](#endnote-2)
1. Program posjeta Uprave za nadzor trgovine obrambenim materijalima (DDTC) tvrtki: Sažeto izvješće, 1. svibnja 2015. do kraja travnja 2016., mrežna stranica DDTC-a, 2016., <http://pmddtc.state.gov/compliance/documents/CVP\_REPORT\_2015-2016.pdf>. Neke obrambene tvrtke vode dnevnike pristupa kojima mogu provjeriti radi li se o „potencijalnim“ ili „stvarnim“ pristupima tehničkim podacima. [↑](#endnote-ref-1)
2. „ITAR Compliance Best Practices Guide“ (Vodič za najbolje prakse usklađenosti s ITAR-om) Aurorait, 2016., <http://aurorait.com/wp-content/uploads/2015/04/ITAR-Compliance-Best-Practices-Guide.pdf>. Ranjivost nultog dana odnosi se na rupu u softveru koja nije poznata ni proizvođaču. Ovu sigurnosnu rupu iskorištavaju hakeri prije nego je proizvođač postane svjestan i pokuša popraviti—ovaj napad se naziva napad nultog dana. „Current Threats: What is a zero day attack?“ („Trenutne prijetnje: što je napad nultog dana?“), Fireeye, 2016., <https://www.fireeye.com/current-threats/what-is-a-zero-day-exploit.html>. [↑](#endnote-ref-2)