**Ostale stavke za razmatranje u namenskoj industriji**

Posebna pitanja od visokog rizika za strana preduzeća koja se bave proizvodima namenske industrije SAD

Vaše preduzeće suočiće se sa nekim jedinstvenim izazovima u pogledu usklađenosti poslovanja kada se bude bavilo proizvodima namenske industrije SAD. Preduzeća moraju da razumeju ograničenja koja se primenjuju na ugradnju/ uključivanje robe poreklom iz SAD i pristup stranih državljana kontrolisanoj robi i tehnologiji poreklom iz SAD. U nastavku su navedeni neki potencijalni problemi sa kojima vaše preduzeće može da se susretne ako se bavi proizvodima namenske industrije SAD.

1. Ukoliko strano preduzeće ugradi deo, komponentu, nastavak ili dodatak koji podleže kontroli u skladu sa Propisom o međunarodnoj trgovini oružjem (ITAR), onda ceo proizvod podleže kontroli u skladu sa ovim propisom. Kompanije stranog odbrambenog sektora treba da budu oprezne kada u svoje gotove proizvode ugrađuju delove, komponente, dodatke i nastavke koji podležu kontroli u skladu sa Propisom o međunarodnoj trgovini oružjem (ITAR), jer na taj način njihovi proizvodi mogu da podležu propisima i nadležnosti kontrola spoljne trgovine strateškom robom SAD (poznato kao **Pravilo transparentnosti**). Preduzeća treba da znaju kako će korišćenje kontrolisanih komponenata u okviru Propisa o međunarodnoj trgovini oružjem (ITAR) uticati na skup kontrola za čije će sprovođenje one biti odgovorne u pogledu gotovih proizvoda.
2. Ako su strani državljani zaposleni u podružnici stranog preduzeća koja se nalazi u SAD, takvim licima neće biti dozvoljen pristup robi vojne namene ili tehničkim podacima koji podležu kontroli u skladu sa Propisom o međunarodnoj trgovini oružjem (ITAR), osim ako se ne pribavi dozvola ili ako se ne primenjuje izuzeće.
3.  Ako strani državljani viši rukovodioci stranog preduzeća putuju u SAD u podružnice svog preduzeća koje se tamo nalaze zbog sastanaka rukovodstva, inspekcija postrojenja i druge potrebe, takvim licima neće biti dozvoljen pristup robi vojne namene ili tehničkim podacima koji podležu kontroli u skladu sa Propisom o međunarodnoj trgovini oružjem (ITAR), osim ako se ne pribavi dozvola ili ako se ne primenjuje izuzeće.
4. Ako državljani SAD zaposleni u podružnici stranog preduzeća koja se nalazi u SAD putuju u strane filijale svog preduzeća, takvim licima neće biti dozvoljeno da sa sobom nose ili razgovaraju o robi vojne namene ili tehničkim podacima koji podležu kontroli u skladu sa Propisom o međunarodnoj trgovini oružjem (ITAR), osim ako se ne pribavi dozvola ili ako se ne primenjuje izuzeće.
5. Ako državljani SAD zaposleni u podružnici stranog preduzeća koja se nalazi u SAD komuniciraju sa zaposlenima koji su strani državljani u stranoj matičnoj kompaniji putem elektronske pošte, telefona, internih dopisa, WebEx sastanaka ili drugih načina elektronske komunikacije, zaposlenima koji su državljani SAD nije dozvoljeno da otkrivaju tehničke podatke koji podležu kontroli u skladu sa Propisom o međunarodnoj trgovini oružjem (ITAR) osim ako se ne pribavi dozvola ili ako se ne primenjuje izuzeće.
6. Ako strano preduzeće proizvodi proizvod koji se nalazi na Listi naoružanja i vojne opreme Sjedinjenih Američkih Država (USML), ako se proizvod otprema u Sjedinjene Američke Države postaje predmet kontrole u skladu sa Propisom o međunarodnoj trgovini oružjem (ITAR) i potpada pod nadležnost Ministarstva spoljnih poslova Sjedinjenih Američkih Država.
7. Ako podružnica stranog preduzeća koja se nalazi u Sjedinjenim Američkim Državama skladišti na svojim računarskim sistemima u SAD (serverima, oblaku, radnim stanicama sistema, laptop računarima i drugim uređajima) tehničke podatke ili softver koji podleže kontroli u skladu sa Propisom o međunarodnoj trgovini oružjem (ITAR), preduzeće mora da primeni firewall da zaštiti sistem sa podacima SAD od računarskih resursa matične kompanije i drugih stranih filijala.
8. Stranim preduzećima nije dozvoljeno da se registruju pri Upravi za kontrolu trgovine naoružanjem i vojnom opremom (DDTC) ili podnesu zahtev za izdavanje dozvole osim ako nisu filijala osnovana u skladu sa zakonom SAD (primenjuju se neka izuzeća, kao što je slučaj podnošenja zahteva za dozvolu za ponovni transfer iz stranih država).
9. Sjedinjene Američke Države takođe imaju posebna pravila koja se primenjuju na zaposlene u matičnoj kompaniji koji imaju dvojno državljanstvo ili državljanstvo treće zemlje. Vaše preduzeće može da odluči da identifikuje državljane trećih zemalja ili one sa dvojnim državljanstvom tokom zasnivanja radnog odnosa (to bi bilo primenljivo u zemljama koje imaju kontrole podrazumevanog izvoza).[[1]](#endnote-1)
10. Gore navedena pravila takođe se primenjuju u slučaju da neko strano preduzeće pripoji američko preduzeće u namenskoj industriji koje se bavi vazduhoplovstvom, satelitima, elektronikom, komunikacijama, bespilotnim letelicama, pomorstvom i drugim delatnostima.

Razmatranja u vezi sa IT i sajber bezbednosti

* Ako vaše preduzeće proizvodi tehnologije u vezi sa naoružanjem ili se bavi istraživanjem i razvojem (R&D) koje obuhvata tehničke podatke ili informacije u vezi sa naoružanjem, preporuka je da vaše preduzeće **uspostavi sofisticirani sistem informatičke i sajber bezbednosti**. Sajber napadi postali su sve sofisticiraniji, i njih sve više sponzorišu odlučne nacionalne države. Kao rezultat toga**, preduzeća koja se bave kontrolisanom tehnologijom moraju aktivno i efektivno da se brane od zlonamernog softvera, virusa i napada nultog dana (zero day attacks)**.[[2]](#endnote-2)

1. DTCC Company Visit Program: Summary Report 1 May 2015 through April 2016, DDTC website, 2016, <http://pmddtc.state.gov/compliance/documents/CVP\_REPORT\_2015-2016.pdf>. Neka preduzeća u namenskoj industriji vode dnevnike pristupa kako bi mogla da provere „potencijalni“ u odnosu na „stvarni“ pristup tehničkim podacima. [↑](#endnote-ref-1)
2. “ITAR Compliance Best Practices Guide,” Aurorait, 2016, <http://aurorait.com/wp-content/uploads/2015/04/ITAR-Compliance-Best-Practices-Guide.pdf>. Ranjivost nultog dana (zero day) odnosi se na rupu u softveru koja nije poznata dobavljaču. Ovu bezbednosnu rupu potom iskorišćavaju hakeri pre nego što dobavljač toga postane svestan i požuri da je popravi - ta zloupotreba naziva se napad nultog dana. “Current Threats: What is a zero day attack?,” Fireeye, 2016, <https://www.fireeye.com/current-threats/what-is-a-zero-day-exploit.html>. [↑](#endnote-ref-2)