**Předběžná tržní konzultace**

Příloha č. 1 „Předmět veřejné zakázky a podmínky plnění“

**Úvod**

Cílem veřejné zakázky je pořízení softwarového nástroje, který bude monitorovat a řídit používání výměnných zařízení a datových nosičů, tj. přístupy k portům (USB, IrDa, Bluetooth, FireWire) koncových stanic v rámci informačního systému ČSSZ, v souladu s požadavky kybernetické bezpečnosti. Využívání softwarového nástroje umožní identifikovat a zabránit připojení nepovolených periferních zařízení k pracovním stanicím, zajistit ochranu před instalací nežádoucích aplikací, eliminovat rizika infikování malware z neautorizovaných USB zařízení a omezit nepovolenou manipulaci s informacemi ČSSZ.

**Otázky v rámci Konzultace:**

1. Bude možné po instalaci nástroje zakázat použití neautorizovaných USB zařízení v rámci informačního systému ČSSZ?
2. Bude možné v navrhovaném řešení rozdělit USB zařízení na dvě kategorie:
   1. USB zařízení, které bude možné využívat pouze v rámci informačního systému ČSSZ;
   2. USB zařízení, které bude možné využívat mimo informační systém (doménu) ČSSZ (například v bankách, OVM, apod.) ?
3. Je možné pomocí nástroje zašifrovat USB zařízení, tak aby byl disk zařízení mimo doménu ČSSZ pouze „read only“ nebo automaticky smazán/konfigurován?
4. Bude možné monitorovat připojená externí zařízení do vnitřní sítě informačního systému ČSSZ?
5. Bude možné zasílat upozornění v reálném čase v případě neoprávněného připojení zařízení?
6. Bude množné využít již zakoupené a využívané USB zařízení nebo bude nutné zakoupit USB zařízení nové vhodné pro navrhované řešení?
7. Bude možné využívat USB zařízení s klávesnicí (např. externí disk chráněný PINem)?
8. Bude možná centrální správa USB zařízení, vytváření podrobného přehledu o USB zařízeních,   
   o připojování USB zařízení do sítě ČSSZ?
9. Budě možná dálková správa USB zařízení?
10. Jak budou stanoveny způsoby a úrovně realizace bezpečnostních opatření a ohodnocení bezpečnostních rizik?
11. Bude prováděno bezpečnostní testování před spuštěním v produkčním prostředí?
12. Bude možné chránit porty koncových stanic před neautorizovaným použitím?
13. Bude možné udělovat výjimky na připojení zařízení ke koncovým stanicím pro vybrané uživatele a dále tyto výjimky spravovat?
14. Bude aplikace přenášet jednoznačný identifikátor uživatele?
15. Budou administrátoři aplikace přistupovat k aplikaci tak, aby mohla být jednoznačně ověřena jejich identita?
16. Budou splněny požadavky kybernetické bezpečnosti vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)?
17. Bude provozní dokumentace vytvořena v souladu s vyhláškou 529/2006 Sb., o požadavcích na strukturu a obsah informační koncepce a provozní dokumentace a o požadavcích na řízení bezpečnosti a kvality informačních systémů veřejné správy (vyhláška o dlouhodobém řízení informačních systémů veřejné správy)?