(3) Subject matter of the contract : Replacing of Concrete Slab of Kusarigawa bridge on Nagano Expressway
(4) Due date for the submission of application forms and relevant documents for the qualification : 4 : 00 P.M. 3 July 2020
(5) Due date for the submission of tenders : 4 : 00 P.M. 11 August 2020.
(6) The language used for application and inquiry shall be Japanese
(7) Contact point for tender documentation : Assistant Manager of Contract Section, General Affairs and Corporate Strategy Department, Hachioji Branch, Central Nippon Expressway Company Limited. 231, Utsugi-Cho, Hachioji, Tokyo, 192―8648 Tel. 042―691―1171

入札公告（建設工事）の変更

次のとおり変更します。
令和２年５月29日
契約責任者　東日本高速道路株式会社
東北支社長　八木　**茂**樹
◎調達機関番号　417　◎所在地番号　04
1　掲載日　令和２年４月23日（号外政府調達第75号）
2　変更内容　29頁４段目、3⑵中、①　交付期間「令和２年４月23日（木）から令和２年５月15日（金）16時00分まで。」を「令和２年４月23日（木）から令和２年６月12日（金）16時00分まで。」に、3⑶中、①　提出期間「令和２年４月23日（木）から令和２年５月15日（金）16時00分まで。」を「令和２年４月23日（木）から令和２年６月12日（金）16時00分まで。」に、3⑷中、①　提出期限「令和２年８月18日（火）16時00分まで。」を「令和２年９月４日（金）16時00分まで。」に、3⑸中、①　開札日時「令和２年８月20日（木）13時30分」を「令和２年９月８日（火）13時30分」に、30頁１段目、5⑷中、Time-limit for the submission of application forms and relevant documents for the qualification:「4:00 P. M. 15 May 2020」を「4:00 P. M. 12 June 2020」に、5⑸中、Time-limit for the submission of tenders:「4:00 P. M. 18 August 2020」を、「4:00 P. M. 4 September 2020」に、それぞれ変更致します。

招　請

資料提供招請に関する公表

次のとおり物品の導入を予定していますので、当該導入に関して資料等の提供を招請します。
令和２年５月29日
東北管区警察局青森県情報通信部長
前田　誠司
◎調達機関番号　009　◎所在地番号　02
○**第１号**
1　調達内容
⑴　品目分類番号　15、28
⑵　導入計画物品及び数量
青森県警察本部用指令通信装置　１式
⑶　調達方法　購入等
⑷　導入予定時期　令和３年度以降
⑸　調達に必要とされる基本的な要求要件
詳細は導入説明書による。
2　資料及びコメントの提供方法
⑴　資料等の提出期限　令和２年６月30日17時15分（郵送の場合は必着のこと。）
⑵　提出先　〒030―0801 青森市新町２―３―１　東北管区警察局青森県情報通信部通信施設課　電話017―723―4211
3　説明書の交付　本公表に基づき応募する供給者に対して導入説明書を交付する。
⑴　交付期間　令和２年５月29日から令和２年６月30日まで。
⑵　交付場所　上記２⑵に同じ。
4　Summary
(1) Classification of the products to be procured : 15, 28
(2) Nature and quantity of the products to be purchased : Command Communications Equipment for Aomori Prefectural Police Headquarters, 1 set
(3) Type of the procurement : Purchase
(4) Basic requirements of the procurement : as enclosure
(5) Time limit for the submission of the requested material : 17 : 15　30 June, 2020
(6) Contact point for the notice : Communications Facilities Section, Aomori Prefectural Info-Communications Department, Tohoku Regional Police Bureau, 2―3―1 Sinmachi Aomori-shi 030―0801 Japan. TEL 017―723―4211

資料提供招請に関する公表

次のとおり特定役務の調達を予定していますので、当該調達に関して資料等の提供を招請します。
令和２年５月29日
日本郵便株式会社調達部担当執行役員
上尾崎幸治
◎調達機関番号　431　◎所在地番号　13
1　調達内容
⑴　品目分類番号　71、27
⑵　調達計画特定役務及び数量　セキュリティ監視業務（マネージドセキュリティサービス）等の委託　一式
⑶　調達方法　購入等
⑷　導入予定時期　令和２年度１月以降
⑸　調達に必要とされる基本的な要求要件
①　24時間365日セキュリティ対策装置のログのリモート監視、相関分析等が行えること。
②　当社のセキュリティ対策装置（外部ＦＷ／ＷＡＦ、内部ＦＷ／ＷＡＦ、外部ＩＤＳ／ＩＰＳ、内部ＩＤＳ／ＩＰＳ等）を監視対象とすること。
③　セキュリティ対策装置の監視に必要な要員、回線、装置類は受託者が用意すること。
④　対象のセキュリティ対策装置及び対象ログ毎に検知可能な脅威（不正アクセス、ウイルス感染、ワーム拡散、コンテンツ改ざん、ＤＤＯＳ等）が明確になっていること。
⑤　公になっていないソフトウエアの脆弱性をつく攻撃、前例のない新しい攻撃手法に対して、一定レベルで検知・対策ができること。
⑥　サイバー攻撃や機器故障等の予兆、事象発生から速やかに初動対応（メール、電話等による分析結果の通知）をすること。
⑦　国内において、セキュリティ監視業務の実績が現在あること。
2　資料及びコメントの提供方法　上記１⑵の特定役務に関する一般的な参考資料及び同⑸の要求要件等に関するコメント並びに提供可能なライブラリーに関する資料等の提供を招請する。
⑴　資料の提供期限　令和２年６月30日午前11時00分（郵送の場合は必着のこと。）
⑵　提出先　〒100―8792 東京都千代田区大手町二丁目３番１号大手町プレイスウェストタワー　日本郵便株式会社調達部（調達戦略担当）担当　竹内　敏章　電話03―3477―0637
3　説明書の交付　本公表に基づき応募する供給者に対して調達説明書を交付する。
⑴　交付期限　令和２年５月29日から令和２年６月29日まで
⑵　交付場所　〒111―8799 東京都台東区西浅草一丁目１番１号　日本郵便株式会社ＩＴ企画部システム運用サービス室（統合運行統制担当）担当　会田　真弘　電話03―5830―0662
4　その他　この導入計画の詳細は調達説明書による。なお、本公表内容は予定であり、変更することがあり得る。
5　Summary
(1) Classification of the services to be procured : 71, 27
(2) Nature and quantity of the services to be required : Outsourcing of managed security services
(3) Type of the Procurement : purchase
(4) Basic requirements of the Procurement :
① 24 hours a day, 365 days a year Ability to remotely monitor logs of security countermeasure devices and perform correlation analysis.
② Our security countermeasure devices (external FW／WAF, internal FW／WAF, External IDS／IPS, internal IDS／IPS, etc.) should be monitored.
③ The trustee must provide the personnel, lines, and equipment necessary for monitoring the security countermeasure device.
④ The threats (illegal access, virus infection, worm spread, content tampering, DDOS, etc.) that can be detected for each security countermeasure device and log are clarified.
⑤ Be able to detect and take measures Against attacks that have software vulnerabilities and new attack methods.