ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΥΠΟΔΟΜΩΝ ΚΑΙ ΜΕΤΑΦΟΡΩΝ
ΓΕΝΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΥΠΟΥΡΓΕΙΟΥ
ΓΕΝΙΚΗ Δ/ΝΣΗ ΟΙΚΟΝΟΜΙΚΩΝ ΥΠΗΡΕΣΙΩΝ
Δ/ΝΣΗ ΠΡΟΜΗΘΕΙΩΝ ΚΑΙ ΛΕΙΤΟΥΡΓΙΚΗΣ ΜΕΡΙΜΝΑΣ
ΤΜΗΜΑ ΔΙΑΓΩΝΙΣΜΩΝ ΚΑΙ ΣΥΜΒΑΣΕΩΝ

Παπάγος, 18-04-2019
Αριθμ. Πρωτ.:29947/2292/ΠΔΕ

Ταχ. Δ/νση : Αναστάσεως & Τσιγάντε
Ταχ. Κώδικας : 101 91 - Παπάγος
Πληροφορίες : Ιωαν. Καραγιώργος
Τηλέφωνο : 210 6508634
e-mail : g.karagiorgos@yme.gov.gr

ΠΡΩΤΟΓΕΝΕΣ ΑΙΤΗΜΑ
ΠΡΟΣΚΛΗΣΗ ΕΚΔΗΛΩΣΗΣ ΕΝΔΙΑΦΕΡΟΝΤΟΣ

Θέμα : «Παροχή υπηρεσιών ελέγχου παρείσδυσης (penetration test) σε πληροφοριακά συστήματα του Υπουργείου Υποδομών και Μεταφορών».

Η Διεύθυνση Προμηθειών & Λειτουργικής Μέριμνας θα προβεί, με τη διαδικασία της απευθείας ανάθεσης, σε παροχή υπηρεσιών ελέγχου παρείσδυσης (penetration test) σε πληροφοριακά συστήματα του Υπουργείου Υποδομών και Μεταφορών, σύμφωνα με τα ακόλουθα στοιχεία:

ΜΟΝΑΔΑ ΦΟΡΕΑ	Διεύθυνση Προμηθειών & Λειτουργικής Μέριμνας
ΑΝΤΙΚΕΙΜΕΝΟ ΤΟΥ ΕΡΓΟΥ	1) Παροχή υπηρεσιών ελέγχου παρείσδυσης (penetration test) σε πληροφοριακά συστήματα του Υπουργείου Υποδομών και Μεταφορών. 2) Παροχή συμβουλευτικών υπηρεσιών, έως εκατό (100) ανθρωποώρες, προς τη Διεύθυνση Πολιτικής Ασφάλειας Υποδομών και Μεταφορών, σε εξειδικευμένα θέματα ασφάλειας πληροφοριακών συστημάτων. **Το ακριβές αντικείμενο των παρεχόμενων υπηρεσιών, το χρονοδιάγραμμα, τα παραδοτέα, η πληρωμή, καθώς και οι τεχνικές απαιτήσεις για τον ανάδοχο περιγράφονται αναλυτικά στα επισυναπτόμενα Παραρτήματα Ι και ΙΙ.**
ΧΡΗΜΑΤΟΔΟΤΗΣΗ	Ε.Ε. 2014ΣΕ57100008 της ΣΑΕ571 (Δαπάνες υλικοτεχνικής στήριξης και επιβλέψεις έργων Οδοποιίας)
ΠΡΟΫΠ/ΣΜΟΣ ΧΩΡΙΣ Φ.Π.Α.	20.000,00€
ΦΠΑ	24%
ΠΡΟΫΠ/ΣΜΟΣ ΜΕ ΦΠΑ	24.800,00€

CPV	72225000-8 : Υπηρεσίες αξιολόγησης και αναθεώρησης της ποιοτικής διασφάλισης των συστημάτων
ΚΡΑΤΗΣΕΙΣ	Τον Ανάδοχο θα βαρύνουν: α) 0,07% υπέρ της Ενιαίας Ανεξάρτητης Αρχής Δημοσίων Συμβάσεων, σύμφωνα με το άρθρο 375 του ν. 4412/2016. β) 0,06% υπέρ της Αρχής Εξέτασης Προδικαστικών Προσφυγών (Α.Ε.Ε.Π.), σύμφωνα με το άρθρο 350 του ν. 4412/2016. γ) Οι ως άνω κρατήσεις υπόκεινται περαιτέρω σε παρακράτηση χαρτοσήμου 3%, σύμφωνα με τα άρθρα 12 και 13 του Κώδικα Τελών Χαρτοσήμου και εισφορά υπέρ ΟΓΑ που αντιστοιχεί σε ποσοστό 20% (σύμφωνα με το ν. 4169/1961).
ΠΑΡΑΚΡΑΤΗΣΗ ΦΟΡΟΥ	Ο νόμιμος φόρος εισοδήματος, σύμφωνα με τις διατάξεις του άρθρου 64 του ν. 4172/2013.
ΥΠΟΒΟΛΗ ΠΡΟΣΦΟΡΩΝ ΚΑΙ ΚΡΙΤΗΡΙΟ ΑΝΑΘΕΣΗΣ	Οι προσφορές θα συνοδεύονται από επιστολή κατάθεσης και θα υποβάλλονται στο Κεντρικό Πρωτόκολλο του Υπ.Υ.Με. (Αναστάσεως 2 και Τσιγάντε στον Παπάγο), σε κλειστό φάκελο, τις εργάσιμες ημέρες και ώρες από 07: 00 έως 14:30. Κριτήριο κατακύρωσης είναι η συμφερότερη από οικονομικής άποψης προσφορά, βάσει τιμής, για το σύνολο του έργου.
ΚΑΤΑΛΗΚΤΙΚΗ ΗΜΕΡΟΜΗΝΙΑ ΚΑΙ ΩΡΑ ΥΠΟΒΟΛΗΣ ΠΡΟΣΦΟΡΩΝ	24-04-2019, ημέρα Τετάρτηκαι ώρα 14:30.
ΔΙΚΑΙΟΛΟΓΗΤΙΚΑ ΓΙΑ ΤΗΝ ΑΝΑΘΕΣΗ ΚΑΙ ΤΗΝ ΕΞΟΦΛΗΣΗ	1. Φορολογική και Ασφαλιστική Ενημερότητα 2. Απόσπασμα Ποινικού Μητρώου σύμφωνα με τον ν. 4412/2016 (Α΄147)
ΚΑΝΟΝΕΣ ΔΗΜΟΣΙΟΤΗΤΑΣ	Η παρούσα ανακοίνωση να αναρτηθεί α) στους δικτυακούς τόπους της Αναθέτουσας Αρχής www.yme.gr και www.ggde.gr και β) στο Κεντρικό Ηλεκτρονικό Μητρώο Δημοσίων Συμβάσεων Κ.Η.Μ.ΔΗ.Σ. **www.eprocurement.gov.gr**

Ο ΓΕΝ. ΓΡΑΜΜΑΤΕΑΣ

ΚΟΙΝΟΠΟΙΗΣΗ

1. Δ/νση Οικονομικής Διαχ/σης (ΔΟΔ)
2. Δ/νση Προϋπολογισμού και Δημοσιονομικών Αναφορών

Α. ΒΟΥΡΔΑΣ

ΑΚΡΙΒΕΣ ΑΝΤΙΓΡΑΦΟ

ΕΣΩΤΕΡΙΚΗ ΔΙΑΝΟΜΗ

1. Χρ. Αρχείο
2. Αθ. Κουτσονίκα
3. Αγλ. Σκρουμπή
4. Ιωαν. Καραγιώργο

ΜΑΓΔΑ ΜΑΚΡΗ

ΠΑΡΑΡΤΗΜΑ Ι

ΕΝΔΕΙΚΤΙΚΟΣ ΣΧΕΔΙΑΣΜΟΣ - ΧΡΟΝΟΔΙΑΓΡΑΜΜΑ - ΠΑΡΑΔΟΤΕΑ – ΠΛΗΡΩΜΗ - ΥΛΟΠΟΙΗΣΗ ΤΟΥ ΕΡΓΟΥ ΠΑΡΟΧΗΣ ΥΠΗΡΕΣΙΩΝ ΕΛΕΓΧΟΥ ΠΑΡΕΙΣΔΥΣΗΣ (PENETRATION TEST) ΣΕ ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ ΤΟΥ ΥΠΟΥΡΓΕΙΟΥ ΥΠΟΔΟΜΩΝ ΚΑΙ ΜΕΤΑΦΟΡΩΝ

Σκοπιμότητα Έργου: Το Έργο σκοπεύει στη διενέργεια ελέγχου παρείσδυσης (penetration test) σε πληροφοριακά συστήματα του ΥΠΥΜΕ, καθώς και στην παροχή συμβουλευτικών υπηρεσιών, έως εκατό (100) ανθρωποώρες, προς τη Διεύθυνση Πολιτικής Ασφάλειας Υποδομών και Μεταφορών, σε εξειδικευμένα θέματα ασφάλειας πληροφοριακών συστημάτων.

Αναλυτικότερα, το αντικείμενο της σύμβασης θα περιλαμβάνει τα παρακάτω:

Α) Διενέργεια δύο (2) penetration tests με χρονική απόσταση περίπου ενός (1) έτους μεταξύ τους, προκειμένου να υλοποιηθούν έγκαιρα οι αναγκαίες διορθωτικές ενέργειες στα πληροφοριακά συστήματα. Ο έλεγχος θα πραγματοποιηθεί τόσο εξωτερικά (remotely) άνευ γνώσης των συστημάτων (black box) όσο και εσωτερικά (internally). Οι έλεγχοι θα υλοποιηθούν σε φάσεις, όπως περιγράφονται κατωτέρω:

1) Συλλογή πληροφοριών (information gathering) για την υποδομή και τους χρήστες του Υπουργείου Υποδομών και Μεταφορών (ΥΠΥΜΕ) με βάση δημόσια διαθέσιμες πηγές (domains, subdomains, IP ranges, DNS, operating systems, employee details κ.λπ.).

2) Σκανάρισμα του δικτύου σε κτήρια του ΥΠΥΜΕ που θα υποδειχθούν από την αρμόδια Διεύθυνση Πολιτικής Ασφάλειας Υποδομών και Μεταφορών, σύμφωνα με την κρισιμότητά τους, για την καταγραφή υπολογιστικών συστημάτων, ανοικτών θυρών και υπηρεσιών (port scanning, TCP/UDP network services, banner grabbing κ.α.).

3) Αναγνώριση ευπαθειών (vulnerability assessment) σε πληροφοριακά συστήματα του ΥΠΥΜΕ (δίκτυα, servers, λειτουργικά συστήματα, εφαρμογές κ.λπ.). Ο έλεγχος των ευπαθειών για τις web εφαρμογές θα αφορά σε έως δέκα (10) εφαρμογές και θα γίνει με βάση το πρότυπο OWASP Top 10 – 2017:

   A1: Injection
   A2: Broken authentication
   A3: Sensitive Data Exposure
   A4: XML External Entities (XXE)
   A5: Broken Access Control
   A6: Security Misconfiguration
   A7: Cross-Site Scripting (XSS)
   A8: Insecure Deserialization
   A9: Using Components with Known Vulnerabilities
   A10: Insufficient Logging and Monitoring

4) Δοκιμή εκμετάλλευσης ενδεχόμενων ευπαθειών που εντοπίστηκαν στο προηγούμενο βήμα (exploitation).

5) Post exploitation: Εύρεση τρόπων βαθύτερης διείσδυσης στο δίκτυο του ΥΠΥΜΕ, καθορισμός των τρόπων διατήρησης του ελέγχου του συστήματος, της αξίας των ευαίσθητων δεδομένων του ΥΠΥΜΕ, καθώς και των μεθόδων διαρροής τους (privilege escalation, pivoting techniques, password hashes, data exfiltration κ.α.).

6) Εξαγωγή αναλυτικού report με όλα τα ευρήματα της διαδικασίας.

Η μεθοδολογία που θα ακολουθηθεί θα πρέπει να βασίζεται σε καθιερωμένα διεθνή πρότυπα και βέλτιστες πρακτικές (π.χ. OWASP, NIST κ.α.).

Β) Παροχή συμβουλευτικών υπηρεσιών προς τη Διεύθυνση Πολιτικής Ασφάλειας Υποδομών και Μεταφορών του ΥΠΥΜΕ σε εξειδικευμένα θέματα ασφάλειας πληροφοριακών συστημάτων (έως 100 ανθρωποώρες κατόπιν αιτήματος).

Η συνολική διάρκεια του έργου θα είναι δέκα έξι (16) μήνες από την υπογραφή της σχετικής σύμβασης.

Γ) Φάσεις – Παραδοτέα

Οι φάσεις και τα παραδοτέα του έργου θα πραγματοποιηθούν ως εξής:

i. <u>Υποέργο 1:</u>

Φάση 1: θα ολοκληρωθεί σε δύο (2) μήνες από την υπογραφή της σχετικής σύμβασης.

Παραδοτέο 1: Πρώτος έλεγχος παρείσδυσης σε πληροφοριακά Συστήματα του ΥΠΥΜΕ. Υποβολή αναλυτικού report στη Διεύθυνση Πολιτικής Ασφάλειας Υποδομών και Μεταφορών.

ii. Φάση 2: θα ξεκινήσει δέκα (10) μήνες από την υπογραφή της σχετικής σύμβασης και θα ολοκληρωθεί σε δύο (2) μήνες.

Παραδοτέο 2: Δεύτερος έλεγχος παρείσδυσης σε πληροφοριακά Συστήματα του ΥΠΥΜΕ. Υποβολή αναλυτικού report στη Διεύθυνση Πολιτικής Ασφάλειας Υποδομών και Μεταφορών.

iii. <u>Υποέργο 2:</u>

Διάρκεια: Καθ' όλη τη διάρκεια της σύμβασης (16 μήνες).

Παραδοτέο 3: Υποβολή αναφοράς με τις καταγεγραμμένες συμβουλευτικές υπηρεσίες προς τη Διεύθυνση Πολιτικής Ασφάλειας Υποδομών και Μεταφορών σε εξειδικευμένα θέματα ασφάλειας πληροφοριακών συστημάτων.

Δ) Οικονομική προσφορά

Οι υποψήφιοι Ανάδοχοι θα πρέπει να συμπληρώσουν στην οικονομική τους προσφορά τιμήματα και για τα δύο (2) υποέργα, σύμφωνα με τον παρακάτω πίνακα:

	Τιμή σε ευρώ χωρίς ΦΠΑ	
	Αριθμητικά	Ολογράφως
Υποέργο 1 (δύο penetration tests με διαφορά περίπου ενός έτους): τίμημα		
Υποέργο 2 (παροχή συμβουλευτικών υπηρεσιών): τίμημα ανά ανθρωποώρα		
ΣΥΝΟΛΟ		

Ε) Πληρωμή

Η πληρωμή του αναδόχου θα γίνει ως εξής:

α) Έξι (6) μήνες από την υπογραφή της σύμβασης: Το 50% της συμβατικής αξίας του υποέργου 1 και το τίμημα που αντιστοιχεί στο σύνολο των ανθρωποωρών που παρασχέθηκαν στο πρώτο εξάμηνο του έργου.

β) Δώδεκα (12) μήνες από την υπογραφή της σύμβασης: Το υπόλοιπο 50% της συμβατικής αξίας του υποέργου 1 και το τίμημα που αντιστοιχεί στο σύνολο των ανθρωποωρών που παρασχέθηκαν στο δεύτερο εξάμηνο του έργου.

γ) Δεκαέξι (16) μήνες από την υπογραφή της σύμβασης: το τίμημα που αντιστοιχεί στις υπολειπόμενες ανθρωποώρες που παρασχέθηκαν στους τελευταίους τέσσερις (4) μήνες του έργου.

ΠΑΡΑΡΤΗΜΑ ΙΙ

ΤΕΧΝΙΚΕΣ ΑΠΑΙΤΗΣΕΙΣ ΓΙΑ ΤΟΝ ΑΝΑΔΟΧΟ

Ο ανάδοχος θα πρέπει να υποβάλει:

1) αναλυτικό βιογραφικό σημείωμα ενός τουλάχιστον μετόχου, διαχειριστή, υπαλλήλου ή μέλους της Ομάδας Έργου, με απαίτηση την κατοχή εξειδικευμένου μεταπτυχιακού διπλώματος σε αντικείμενο κυβερνοασφάλειας (cyber security),

2) πίνακα με τουλάχιστον δύο (2) ολοκληρωμένα έργα penetration test που διενεργήθηκαν από αυτόν κατά τη διάρκεια των τελευταίων δώδεκα μηνών, που θα συνοδεύεται από πιστοποιητικό / βεβαίωση του αναθέτοντος Οργανισμού και στο οποίο θα περιγράφεται αναλυτικά το αντικείμενο και θα βεβαιώνεται ότι αυτό πραγματοποιήθηκε έντεχνα, εμπρόθεσμα και σύμφωνα με τις συμβατικές υποχρεώσεις,

3) πίνακα με βεβαιώσεις διενέργειας τουλάχιστον εκατό (100) ωρών εκπαίδευσης σε θέματα ασφάλειας πληροφοριακών συστημάτων κατά τη διάρκεια των τελευταίων δώδεκα μηνών, υπό την αιγίδα αναγνωρισμένων Δημόσιων Φορέων (Α.Ε.Ι., Α.Τ.Ε.Ι., Ι.Ε.Κ., Κ.Ε.Κ., Ο.Α.Ε.Δ.).