MARKAS BESAR TNI ANGKATAN DARAT
PUSAT SANDI DAN SIBER

KERANGKA ACUAN KERJA / *TERM OF REFERENCE*
MATERIEL PUSSANSIAD *CYBER PERSONAL EQUIPMENT TOOLS* TA 2023

Kementerian Negara/Lembaga	:	Kementerian Pertahanan
Unit Eselon-I/II	:	TNI AD
Program	:	Program Modernisasi Alutista dan Non Alutista/Sarana dan Prasarana Matra Darat
Sasaran Program	:	Terwujudnya kesiapan operasional Non-Alutista dan Faslat Pendukung
Indikator Kinerja Program	:	Persentase kesiapan operasional Non-Alutista dan Faslat pendukung TNI AD
Kegiatan	:	Pengadaan/Penggantian Material Non Alutista
Sasaran Kegiatan	:	Terwujudnya kesiapan Matsus untuk mendukung operasi, latihan, dan pendidikan
Indikator Kinerja Kegiatan	:	Persentase kesiapan Matsus untuk mendukung operasi, latihan, dan pendidikan
Klasifikasi Rincian *Output* (KRO)	:	Sarana Bidang Pertahanan dan Keamanan
Indikator KRO	:	Terwujudnya Dukungan Pengadaan/Penggantian Materiil Non Alutsista
Rincian *Output* (RO)	:	Dukungan Pengadaan/Penggantian Materiil Non Alutsista
Indikator RO	:	Pengadaan/Penggantian Materiel Non Alutsista
Volume RO	:	1
Satuan RO	:	Paket
Komponen	:	Melaksanakan Pengadaan/Penggantian Materiel Non Alutsista
Sub Komponen	:	Materiel Pussansiad
Indikator Sub Komponen	:	Persentase pemenuhan Matpussansiad sesuai TOP/DSPP
Volume Sub Komponen	:	1
Satuan Sub Komponen	:	Paket

A. Latar Belakang.

1. Dasar Hukum.

   a. Peraturan Menteri Pertahanan RI Nomor 38 tahun 2012 tanggal 26 Desember 2012 tentang Sistem Perencanaan Pembangunan Pertahanan Negara (SPP Hanneg);

b. Peraturan Kasad Nomor Perkasad/64/XII/2013 tanggal 30 Desember 2013 tentang Revisi Pembangunan Jangka Panjang (RPJP) TNI AD tahun 2015-2024;

c. Peraturan Kasad Nomor Perkasad/50/IX/2013 tanggal 17 September 2013 tentang Revisi Pembangunan Kekuatan Pokok Minimum (Minimum Essential Force) Angkata Darat Tahun 2010-2029;

d. Peraturan Kasad Nomor 26 Tahun 2019 tanggal 26 Desember 2019 tentang Organisasi dan Tugas Pusat Sandi dan Siber TNI Angkatan Darat (Orgas Pussansiad);

e. Surat Kasad Nomor B/4563/XII/2019 tanggal 13 Desember 2019 tentang Renbugar prioritas pembangunan kemampuan Siber TNI AD tahun 2020-2024;

f. Keputusan Danpussansiad Nomor Kep/479/XII/2022 tanggal 16 Desember 2022 tentang Program Kerja dan Anggaran Pussansiad TA 2023; dan

g. Pertimbangan Komandan dan Staf Pussansiad.

2. Gambaran Umum.

a. Perkembangan IT yang sangat masif memberikan dampak pada permasalahan keamanan yang merupakan salah satu faktor penting dan harus diperhatikan dalam membangun sebuah sistem, aplikasi maupun website. Permasalahan keamanan tersebut menjadi sebuah tantangan tersendiri bagi para pengguna internet, karena tidak ada jaminan yang pasti akan defenisi aman maupun terlindungi dari serangan itu sendiri. Dalam perkembangannya, tidak ada sistem yang benar-benar aman, bukanlah sebuah pernyataan semata, namun telah dirasakan dalam realitas semua pengguna internet. Sebuah tindakan yang wajar diambil oleh setiap user untuk menjaga keamanan informasi dengan segera dilakukannya kegiatan atau metode penetration test (pentest). Pengujian ini berfungsi untuk menguji seberapa handal pertahanan keamanan informasi dari perangkat maupun sistem IT yang digunakan. Ketika dari hasil pentest terbukti bahwa masih terdapat celah pada keamanan informasi, maka tindakan selanjutnya adalah melakukan penutupan pada celah yang ditemukan sebelum terjadi serangan yang sesungguhnya dari para hackers atau potensi lawan;

b. Penggunaan IT juga memberikan celah pada tiap-tiap instansi dan lembaga dengan celah keamanan sistem informasi. Indonesia menjadi target mudah bagi para hackers dibuktikan dengan banyaknya serangan yang terjadi. Indonesia mencatat terdapat 12.895.554 jumlah total serangan siber dan 513.863 jumlah total serangan malware dengan sumber serangan tertinggi berasal dari Rusia, China dan Amerika Serikat yang diambil rentang

waktu 2019 sampai dengan 2020 yang dideteksi menggunakan 22 sensor aktif tersebar di 6 sampai 9 provinsi di Indonesia. Contoh serangan siber paling umum adalah malicious codes, viruses, worms dan trojans, malware, malicious insiders, stolen devices, phishing, social engineering dan serangan berbasis web. Adapun contoh serangan berbasis web secara umum yang paling sering dilancarkan, seperti Structured Query Language (SQL) Injection, Distributed Denial of Service (DDoS), Cross Site Scripting (XSS), Defacement, Account Hijacking, dan Malware;

c. Celah kerentanan merupakan kelemahan terhadap suatu aset yang dapat dimanfaatkan oleh satu atau lebih ancaman dimana aset tersebut memiliki nilai dalam suatu organisasi, operasional, dan kelangsungan fungsional termasuk sumber daya informasi yang mendukung misi organisasi. Kerentanan didefinisikan sebagai cacat atau kelemahan dalam prosedur keamanan sistem, perancangan, implementasi, atau pengendalian internal yang dapat dilakukan (sengaja dipicu atau sengaja dieksploitasi) dan mengakibatkan pelanggaran keamanan atau pelanggaran terhadap kebijakan keamanan sistem. Pusat Sandi dan Siber TNI AD (Pussansiad) sebagai salah satu leading sektor bidang pertahanan dan keamanan siber di Indonesia bertugas penting dalam melakukan penetration testing guna melindungi dari setiap potensi ancaman dan potensi lawan di lingkungannya maupun yang terhubung dengan Mabes TNI. Pussansiad memerlukan alat uji untuk melakukan pengujian keamanan informasi dimana seorang asesor bertugas untuk menguji celah keamanan apabila terjadi serangan dan untuk mengidentifikasi metode peretasan fitur keamanan aplikasi, sistem, atau jaringan. Alat ini merupakan kebutuhan prioritas yang dapat menggunakan serangan yang nyata, sistem yang nyata, dan data yang nyata menggunakan alat dan teknik yang sering dipakai oleh seorang hackers sehingga diketahui celah keamanan mana yang menjadi prioritas untuk dilindungi. Pentest biasanya dilakukan bersamaan dengan Vulnerability Assessment (VA). VA sangatlah dibutuhkan oleh Pussansiad sebagai sebuah proses untuk mengidentifikasi risiko dan celah kerentanan pada aplikasi, sistem, ataupun jaringan. Sebagian besar pentest mencari kombinasi kerentanan pada satu atau lebih sistem untuk mendapatkan akses lebih dalam pada sistem yang menjadi target dibandingkan dengan hanya mengetahui satu macam kerentanan; dan

d. Dalam implementasinya, kebutuhan prioritas tersebut menjadi sangat berguna bagi Pussansiad antara lain untuk menentukan seberapa baik sebuah sistem dapat menangani serangan dunia maya. Selain itu dapat menentukan penanggulangan yang dapat mengurangi ancaman terhadap sistem, dan untuk meningkatkan keamanan pada aplikasi, sistem, atau jaringan yang dimiliki. Kebutuhan alat tersebut juga digunakan untuk mendeteksi serangan dan merespon dengan cepat dan tepat. Kebutuhan tersebut merupakan suatu kebutuhan prioritas mengingat serangan siber yang semakin hari semakin massif. Kebutuhan alat ini secara garis besar

bertujuan untuk menganalisis risiko yang akan timbul dengan adanya kerentanan yang telah diidentifikasi pada tahap vulnerability assessment dan memberikan rekomendasi tindakan yang perlu dilakukan apabila sistem yang diuji dapat lolos dari serangan hackers Usaha pertahanan negara mempertimbangkan dinamika perkembangan lingkungan strategis regional dan internasional. Perkembangan lingkungan strategis saat ini mengarah kepada ancaman yang semakin kompleks dan multidimensional, sementara itu kemampuan pertahanan dan keamanan saat ini dihadapkan pada situasi kekurangan jumlah dan ketidaksiapan alutsista dan alat utama non alutsista lainnya yang jika tidak dilakukan upaya percepatan penggantian, peningkatan, dan penguatan akan menyulitkan penegakan kedaulatan negara, penyelamatan bangsa, dan penjagaan keutuhan wilayah di masa mendatang, maka perlu diadakan kajian guna memberikan alternatif pemilihan teknologi yang tepat sehingga dapat dimanfaatkan secara optimal oleh TNI Angkatan Darat dalam memilih dan menentukan alat web vulnerability assessment yang sesuai dengan kebutuhan untuk tercapainya tugas pokok Pussansiad TNI AD.

B. **Penerima Manfaat.** Penerima manfaat kegiatan pengadaan *Cyber Personal Equipment Tools* adalah satuan Pussansiad.

C. **Strategi Pencapaian Keluaran.**

1. Metode Pelaksanaan. Kegiatan pengadaan *Cyber Personal Equipment Tools* dilaksanakan secara Kontraktual.

2. Tahapan dan Waktu Pelaksanaan.

   a. Tahapan Kegiatan. Tahapan proses yang akan dilalui terdiri dari:

      1) Tahap Perencanaan.
         a) Melaksanakan survei dan mengumpulkan data tentang *Cyber Personal Equipment Tools* yang akan dilaksanakan sebagai bahan acuan proses pengadaan; dan
         b) Melaksanakan analisa tentang biaya pengadaan *Cyber Personal Equipment Tools*.

      2) Tahap Persiapan.
         a) Merencanakan kebutuhan pengadaan *Cyber Personal Equipment Tools* sesuai hasil survei/pengumpulan data; dan
         b) Menyusun RAB.

      3) Tahap Pelaksanaan. Dilaksanakan sebagai prosedur dan ketentuan pengadaan barang dan jasa di lingkungan TNI AD.
         a) Tender.
            (1) Pengumuman tender;
            (2) Penjelasan tender kepada penyedia barang;

(3) Pembukaan penawaran;
(4) Penunjukan pemenang tender; dan
(5) Surat perjanjian/kontrak.

b) Pengiriman barang;
c) Pemeriksaan barang; dan
d) Pembayaran kepada penyedia barang.

4) Pengakhiran. Dilaksanakan evaluasi guna memperoleh gambaran yang realistis dilanjutkan penyusunan laporan pelaksanaan kegiatan.

b. Waktu Pelaksanaan Kegiatan.

NO	KEGIATAN	TA 2023									KET
		I	II	III	IV	V	VI	VII	VIII	IX	
1.	Tahap Perencanaan										
2.	Tahap Persiapan										
3.	Tahap Pelaksanaan										
4.	Tahap Pengakhiran										

D. **Kurun Waktu Pencapaian Keluaran**. Kegiatan pengadaan *Cyber Personal Equipment Tools* dicapai mulai dari bulan Februari sampai dengan September TA 2023.

E. **Biaya yang diperlukan. Biaya yang dikeluarkan untuk** pengadaan *Cyber Personal Equipment Tools* sebesar Rp.31.765.630.000,00. (Tiga puluh satu miliar tujuh ratus enam puluh lima juta enam ratus tiga puluh ribu rupiah).

Komandan Pusat Sandi dan Siber TNI AD,

Iroth Sonny Edhie
Brigadir Jenderal TNI