TỔNG CÔNG TY HÀNG KHÔNG VIỆT NAM	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: ……/TCTHK-CĐSCN	*Hà Nội, ngày 11 tháng 4 năm 2025*

V/v cung cấp giải pháp và chào giá.

Kính gửi: …….

Tổng công ty Hàng không Việt Nam (TCTHK) xin gửi tới Quý Công ty lời chào trân trọng.

Hiện nay TCTHK đang có nhu cầu triển khai gói dịch vụ "Thuê tư vấn triển khai, hạ tầng tích hợp chức năng Check-in trên ứng dụng VNeID" và "Dịch vụ xác thực sinh trắc học với Trung tâm RAR". Chi tiết yêu cầu về dịch vụ tại các Phụ lục đính kèm.

TCTHK kính đề nghị Quý Công ty cung cấp giải pháp, chào giá và khả năng triển khai thực hiện. Yêu cầu: Hoàn thành việc triển khai tất cả các hạng mục trước ngày 30/4/2025.

Đầu mối liên hệ của TCTHK:

- Ông Vũ Đức Quân, Phó Trưởng phòng Quản trị Chuyển đổi số;
- Địa chỉ Email: quanvuduc@vietnamairlines.com;
- Số điện thoại: 0913 528 883./.

Trân trọng cảm ơn sự hợp tác!

Nơi nhận: - Như trên; - TGĐ (b/c); - Phó TGĐ ĐV Tuấn (b/c); - TB CĐSCN (b/c); - Lưu VT CĐSCN.	**TL. TỔNG GIÁM ĐỐC** **KT. TRƯỞNG BAN CĐSCN** **PHÓ TRƯỞNG BAN** **Hoàng Ngọc Chí**

PHỤ LỤC 01
PHẠM VI CÔNG VIỆC

DỊCH VỤ TƯ VẤN KỸ THUẬT VÀ ĐÁNH GIÁ AN TOÀN THÔNG TIN

I. Tư vấn và hỗ trợ thiết kế giải pháp

- Khảo sát nhu cầu của Vietnam Airlines trong việc kết nối hệ thống xác thực và định danh điện tử VNeID.
- Tư vấn thiết kế giải pháp phù hợp với nhu cầu của Vietnam Airlines và đồng thời phù hợp với hiện trạng cung cấp dịch vụ của RAR - Trung tâm nghiên cứu, ứng dụng dữ liệu dân cư và căn cước công dân, tuân thủ đầy đủ và nghiêm chỉnh Nghị định 69 về Định danh và xác thực điện tử.
- Hỗ trợ trong quá trình Vietnam Airlines xây dựng Tài liệu giải pháp và Mô hình kiến trúc hạ tầng.
- Các dịch vụ tư vấn và hỗ trợ Vietnam Airlines thiết kế giải pháp, bao gồm:

STT	Dịch vụ do Trung tâm RAR – C06 cung cấp	Luồng nghiệp vụ ứng dụng của Vietnam Airlines
1	Dịch vụ đăng nhập bằng tài khoản VNeID (SSO)	- Mua vé máy bay trên ứng dụng VNeID
2	Dịch vụ chia sẻ thông tin	- Làm thủ tục bay trên ứng dụng VNeID
3	Dịch vụ xác thực khuôn mặt (Face Verification)	
4	Dịch vụ xác thực chống giả mạo khuôn mặt (LivenNCC Detection)	

II. Tư vấn và hỗ trợ hoàn thiện hồ sơ, thủ tục

- Hỗ trợ chuẩn bị bộ hồ sơ, phương án khai thác sử dụng dịch vụ xác thực điện tử.
- Hỗ trợ chuẩn bị và hoàn thiện Hợp Đồng khai thác dịch vụ.
- Hỗ trợ chuẩn bị hồ sơ để nghiệm thu dịch vụ trên môi trường dev/test và môi trường production.
- Hỗ trợ thúc đẩy quá trình ký Hợp Đồng và xin cấp phép kết nối dịch vụ.

III. Tư vấn, hỗ trợ trong quá trình triển khai, nâng cấp các phương án an toàn thông tin

- Khảo sát hệ thống và các phương án an toàn thông tin hiện có của Vietnam Airlines.
- Tư vấn triển khai các phương án an toàn thông tin cho các hệ thống sử dụng dịch vụ xác thực và khai thác danh tính điện tử theo yêu cầu của C06.
- Kiểm tra khả năng đáp ứng an toàn thông tin hệ thống của Vietnam Airlines theo các tiêu chí do C06 hướng dẫn.
- Đưa ra các khuyến nghị, cảnh báo và đề xuất giải pháp khắc phục cho Vietnam Airlines.
- Hỗ trợ trong quá trình Vietnam Airlines thực hiện nâng cấp hệ thống.
- Kiểm tra lại sau khi Vietnam Airlines thực hiện khắc phục.
- Hỗ trợ Vietnam Airlines trong suốt quá trình C06 kiểm tra an toàn thông tin hệ thống.

PHỤ LỤC 02
PHẠM VI DỊCH VỤ CHO THUÊ MÁY CHỦ, THIẾT BỊ, HẠ TẦNG VÀ GIẢI PHÁP AN TOÀN THÔNG TIN

I. Bàn giao, lắp đặt, triển khai máy chủ, thiết bị, hạ tầng

- Đối với việc cung cấp thiết bị HSM**:** trong vòng 07 ngày làm việc kể từ ngày Hợp đồng này được ký kết, NCC có trách nhiệm bàn giao thiết bị HSM theo đúng số lượng, chủng loại, thông số kỹ thuật được quy định tại Mục III, Phụ lục 02 đính kèm.
- Đối với dịch vụ thuê hạ tầng giải pháp và dịch vụ đảm bảo ANAT**:** trong vòng 07 ngày làm việc kể từ ngày Hợp đồng có hiệu lực, NCC có trách nhiệm thiết kế, lắp đặt và cài đặt Máy chủ và tiến hành bàn giao quyền truy cập vào Máy chủ cho Vietnam Airlines. NCC có trách nhiệm duy trì hỗ trợ kỹ thuật đảm bảo hệ thống Máy chủ hoạt định ổn định.

II. Cấu hình thiết bị

1. Giai đoạn thí điểm

Tên thiết bị	Thông số	Số lượng	Mô tả
1. Thiết bị trung gian			
Máy chủ Agent GW	CPU 32 Core RAM 128 GB SSD 1TB	2	Ứng dụng xử lý và kết nối đến trung gian xác thực
Thiết bị HSM	Thales A750 - RSA - 2048 signing ops: 5000 - ECC P256 signing ops: 10000 - AES - GCM small packet encryption ops: 10000	2	Thiết bị mã hóa dữ liệu
Thiết bị Cân bằng tải	L7 requests per second: 1.8M L4 connections per second: 750K L4 HTTP requests per second: 3.5M Maximum L4 concurrent connections: 38M Throughput: 50 Gbps/40 Gbps L4/L7	1	Cân bằng tài cho Agent GW và API HSM
2. Giải pháp và dịch vụ ATTT			

Tên thiết bị	Thông số	Số lượng	Mô tả
Web Application Firewall	L7 requests per second: 1.8M L4 connections per second: 750K L4 HTTP requests per second: 3.5M Maximum L4 concurrent connections: 38M Throughput: 50 Gbps/40 Gbps L4/L7	1	Tường lửa ứng dụng web bảo vệ API
NGFW (bao gồm license Threat Prevention)	Firewall Throughput: 9.5 Gbps Threat Prevention Throughput: 6.2 Gbps IPsec VPN throughput: 5.6 Gbps Max concurent sNCCion: 192,000 New sNCCion per second: 13,100	1	Tường lửa thế hệ mới bảo vệ truy cập trái phép, DDOS, mã độc
Phần mềm giám sát hạ tầng	Giám sát hiệu năng CPU, RAM, disk, interface.	1	Phần mềm giám sát hiệu năng hoạt động các các thiết bị và cảnh báo.
3. Cơ sở hạ tầng			
Hạ tầng thiết bị mạng			Các thiết bị chuyển mạch Core, Distributed, Management.
Hạ tầng DataCenter			Hạ tầng điện, chống cháy, rack, …
Kênh truyền Internet	200 MB trong nước, 20 MB quốc tế	1	Kênh truyền dành cho kết nối VPN tới VNA CLOUD DATACENTER và C06

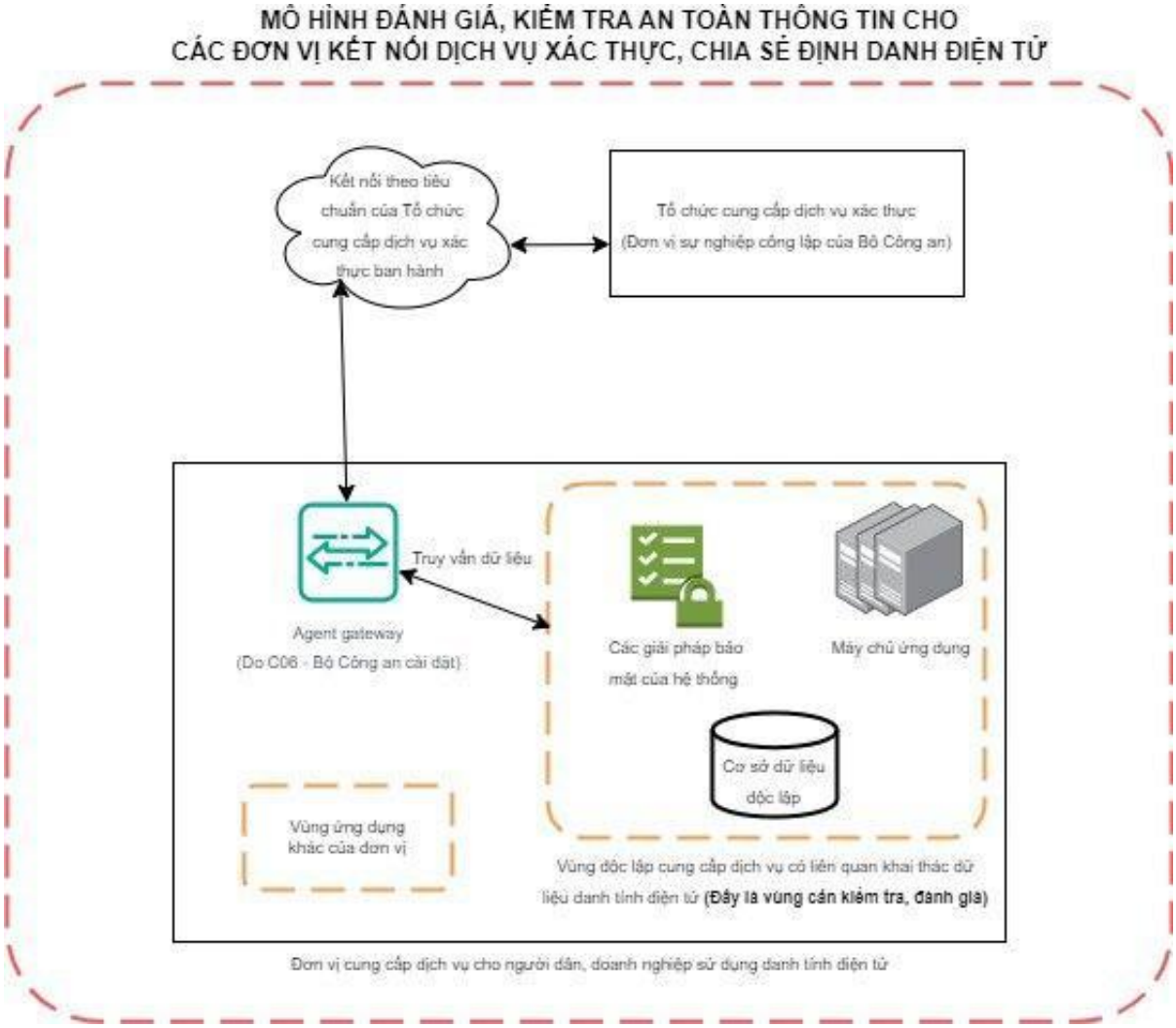
2. Giai đoạn chạy toàn quốc

Tên thiết bị	Thông số	Số lượng	Mô tả
1. Thiết bị trung gian			
Máy chủ Agent GW	CPU 32 Core RAM 128 GB SSD 1TB	2	Ứng dụng xử lý và kết nối đến trung gian xác thực
Thiết bị HSM	Thales A750 - RSA - 2048 signing ops: 5000 - ECC P256 signing ops: 10000 - AES - GCM small packet encryption ops: 10000	2	Thiết bị mã hóa dữ liệu
Thiết bị Cân bằng tải	L7 requests per second: 1.8M L4 connections per second: 750K L4 HTTP requests per second: 3.5M Maximum L4 concurrent connections: 38M Throughput: 50 Gbps/40 Gbps L4/L7	2	Cân bằng tài cho Agent GW và API HSM
Máy chủ Agent GW	CPU 32 Core RAM 128 GB SSD 1TB	2	Ứng dụng xử lý và kết nối đến trung gian xác thực
2. Giải pháp và dịch vụ ATTT			
Web Application Firewall	L7 requests per second: 1.8M L4 connections per second: 750K L4 HTTP requests per second: 3.5M Maximum L4 concurrent connections: 38M Throughput: 50 Gbps/40 Gbps L4/L7	2	Tường lửa ứng dụng web bảo vệ API
NGFW (bao gồm license Threat Prevention)	Firewall Throughput: 20.8/16.9 Gbps Threat Prevention Throughput: 7.6/8.7 Gbps Max sNCCion: 2M	2	Tường lửa thế hệ mới bảo vệ truy cập trái phép, DDOS, mã độc

Tên thiết bị	Thông số	Số lượng	Mô tả
	New sNCCion per second: 205000		
Dịch vụ giám sát hạ tầng	Giám sát hiệu năng CPU, RAM, disk, interface.	1	Giám sát 24/7
Dịch vụ giám sát an toàn thông tin	Giám sát sự kiện, cảnh báo tấn công	1	Giám sát 24/7
Dịch vụ quản lý truy cập PAM	Cung cấp dịch vụ truy cập an toàn qua PAM khi quản trị Database và thiết bị HSM, AgentGW	1	
Dịch vụ rà quét và nâng cấp lỗ hổng ANAT định kỳ	Định kỳ rà quét mỗi 3 tháng và nâng cấp ANAT cho hệ thống	1	
Dịch vụ quản trị vận hành		1	Quản trị vận hành hệ thống, cấu hình an toàn.
3. Cơ sở hạ tầng			
Hạ tầng thiết bị mạng			Các thiết bị chuyển mạch Core, Distributed, Management.
Hạ tầng DataCenter			Hạ tầng điện, chống cháy, rack, …
Kênh truyền BGP	200 MB trong nước, 20 MB quốc tế	2	Kênh truyền dành cho kết nối VPN tới VNA CLOUD DATACENTER và C06. Đảm bảo độ sẵn sàng rất cao.

PHỤ LỤC 03
NỘI DUNG KIỂM TRA KHẢ NĂNG ĐÁP ỨNG AN TOÀN THÔNG TIN

I. MÔ HÌNH ĐÁNH GIÁ



II. CÁC TIÊU CHÍ ĐÁNH GIÁ

1. Về hồ sơ đề xuất cấp độ và các phương án triển khai

STT	Hạng mục các phương án ATTT cho các hệ thống sử dụng dịch vụ xác thực và khai thác danh tính điện tử	
1	Có phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập	Tường lửa; hệ thống IDS/IPS.
2	Có phương án phòng, chống tấn công mạng cho web app API service	Tường lửa ứng dụng Web.
3	Có phương án chặn lọc phần mềm độc hại trên môi trường mạng	Giải pháp/Thiết bị phát hiện và ngăn chặn mã độc lớp mạng.
4	Có phương án quản lý phần mềm phòng chống mã độc trên các máy chủ/máy tính người dùng vận hành quản trị.	Đầu tư giải pháp AntiVirus có chức năng quản lý tập trung hoặc hệ thống EDR.

STT	Hạng mục các phương án ATTT cho các hệ thống sử dụng dịch vụ xác thực và khai thác danh tính điện tử	
5	Có kế hoạch kiểm tra đánh giá An toàn thông tin định kỳ hàng năm.	(1) Rà quét lỗ hổng bảo mật (Vulnerability assNCCment) (2) Kiểm thử App/Service (3) Kiểm tra tiêu chuẩn cấu hình an toàn (Audit)

2. Các tiêu chí đánh giá ATTT trong quá trình kiểm tra

STT	Yêu cầu	
I	**Phạm vi kiểm tra lỗ hổng bảo mật**	
1	**Rà soát kiểm tra lỗ hổng bảo mật của hệ thống máy chủ**	
1.1	**Tiêu chuẩn đánh giá**	Đánh giá được thực hiện dựa trên bộ tiêu chuẩn PTES (Penetration Testing Execution Standard) đây là bộ tiêu chuẩn uy tín áp dụng cho kiểm tra đánh giá bảo mật hệ thống máy chủ, máy tính, thiết bị và dịch vụ được các tổ chức, chính phủ và doanh nghiệp tin dùng.
	Lên kịch bản, các phương án đánh giá	Xác định và thống nhất thành phần cần thực hiện kiểm tra, các hướng tiếp cận ứng với từng phạm vi cụ thể, lập kế hoạch dò quét và kiểm tra. Chuẩn bị các tài nguyên, công cụ cần thiết ứng với các mục tiêu trong phạm vi kiểm tra.
	Thu thập thông tin	Thu thập thông tin là giai đoạn đầu tiên trong quá trình kiểm tra đánh giá mà ở đó các kỹ sư của nhà cung cấp sẽ cố gắng thu thập nhiều nhất có thể các thông tin về mục tiêu để hỗ trợ cho công việc tìm kiếm và khai thác lỗ hổng bảo mật sau này. Ở một mức độ rộng nhất trong phạm vi kiểm tra đánh giá thông tin này sẽ bao gồm thông tin về nhân viên, cơ sở vật chất, các sản phẩm và kế hoạch, các thông tin bí mật, riêng tư hoặc tất cả các thông tin liên quan đến mục tiêu.
	Phân tích, nhận dạng điểm yếu	Phân tích lỗ hổng bảo mật được sử dụng để đánh giá các rủi ro xảy ra đối với các lỗ hổng bảo mật tồn tại. Công việc phân tích lỗ hổng bảo mật được chia làm 2 phần. Nhận dạng lỗ hổng bảo mật và xác nhận lại sự tồn tại của lỗ hổng trên hệ thống. Nỗ lực tìm kiếm lỗ hổng bảo là công việc chính trong giai đoạn nhận dạng lỗ hổng. Xác nhận lại sự tồn tại của lỗ hổng sẽ làm giảm số lượng các lỗ hổng trong phần nhận dạng và chỉ giữ lại các lỗ hổng nào thực sự hợp lệ. Thu thập thông tin CVE trên hệ thống, thực hiện kiểm tra khả năng khai thác của các CVE này.
1.2	**Báo cáo**	Tất cả các kết quả kiểm tra, bằng chứng lỗ hổng, phương pháp chứng minh các lỗ hổng bảo mật đều phải được ghi nhận một cách chi tiết và đầy đủ. Báo cáo phải rõ ràng, ngắn gọn và được tổ chức tốt, cho phép các bên liên quan hiểu được tình hình bảo mật và thực hiện các hành động thích hợp để giải quyết các rủi ro đã xác định.
1.3	**Hỗ trợ kỹ thuật**	Đội ngũ kỹ sư đánh giá bảo mật sẽ phối hợp cùng đội ngũ cán bộ

		kỹ thuật của đơn vị để tư vấn các phương án xử lý lỗ hổng bảo mật, cập nhật bản vá. Sau quá trình xử lý lỗ hổng, các kỹ sư hỗ trợ xác minh, đánh giá lại trạng lại của các lỗ hổng bảo mật đã được phát hiện trước đó.
2	**Rà soát bảo mật ứng dụng API và Web Services**	
2.1	**Tiêu chuẩn sử dụng**	Đánh giá được thực hiện dựa trên bộ tiêu chuẩn OWASP Top 10 và OWASP Testing Guide. Đây là bộ tiêu chuẩn uy tín áp dụng cho kiểm tra đánh giá bảo mật ứng dụng, được các tổ chức, chính phủ và doanh nghiệp tin dùng.
	Thu thập thông tin	Các kỹ thuật kiểm tra sẽ được sử dụng để thu thập càng nhiều thông tin càng tốt về ứng dụng. Thu thập thông tin được thực hiện thông qua các công cụ tìm kiếm và các thông tin kỹ thuật được tiết lộ bởi ứng dụng.
	Kiểm tra quản lý cấu hình và triển khai	Trong phần này, quá trình kiểm tra được thiết kế để xác nhận về khả năng tồn tại các lỗ hổng trong các cấu hình của nền tảng công nghệ và mô hình ứng dụng, chính sách cấu hình ứng dụng
	Kiểm tra quản lý định danh	Trong phần này, quá trình kiểm tra được thiết kế để có thể tìm ra các lỗ hổng về việc xác định sai các quyền hạn của người sử dụng trong ứng dụng.
	Kiểm tra cơ chế xác thực	Các kiểu kiểm tra được thiết kế để xác nhận các cơ chế bảo mật liên quan đến việc quản lý xác thực trong ứng dụng. Quá trình kiểm tra sẽ đánh giá về bảo mật dữ liệu, quá trình đăng nhập, đặt lại mật khẩu và các vấn đề liên quan tới chứng thực.
	Kiểm tra cơ chế phân quyền	Phần kiểm tra này là để xác nhận về kiểm soát truy cập: đánh giá khả năng một người sử dụng bình thường khi truy cập tài nguyên, chức năng hoặc thông tin của ứng dụng không thuộc sở hữu của chính họ và khả năng truy cập vào các vai trò (accNCC role) hoặc mức độ cụ thể của các đặc quyền khác với quyền được cấp bởi ứng dụng.
	Kiểm tra quản lý phiên	Yếu tố quan trọng nhất của một ứng dụng web là cách ứng dụng quản lý những phiên làm việc của người sử dụng. Phần này bao gồm tất cả các kiểm tra về quá trình khởi tạo, quản lý và kết thúc phiên làm việc của người sử dụng.
	Kiểm tra sàng lọc dữ liệu đầu vào	Một trong những điểm chính của bảo mật ứng dụng nằm trong sự quản lý dữ liệu nhập vào của người dùng trong quá trình sử dụng ứng dụng. Các lỗ hổng trong phần này thường gây ra các lỗ hổng ảnh hưởng rất lớn đến các ứng dụng web, chẳng hạn như SQL injection, HTML injection, XSS, XML-PATH, File Inclusion, lỗi tràn bộ đệm…
	Kiểm tra cơ chế xử lý lỗi	Phần này tập trung vào khả năng xử lý lỗi của ứng dụng. Các kiểm tra đã được thực hiện bao gồm thay đổi các dữ liệu nhập vào ứng dụng ở các trạng thái thừa, thiếu, sai định dạng dữ liệu để xác định tra khả năng chống lỗi của ứng dụng.
	Kiểm tra sử dụng mật mã học	Phần này tập trung vào việc kiểm tra các cơ chế mã hóa được dùng trong ứng dụng. Các biện pháp kiểm thử được thực hiện để

		đảm bảo rằng việc mã hóa không thể bị phá vỡ, không có cơ chế mã hóa yếu được sử dụng.
	Kiểm tra Logic nghiệp vụ ứng dụng	Mục đích của phần này là để kiểm tra các quy trình hoat động trong ứng dụng. Trong bảo mật ứng dụng, ngoài các lỗ hổng kỹ thuật, các lỗi thiết kế của ứng dụng cũng có thể gây ra các hậu quả nghiêm trọng, việc tuân thủ quy trình hoạt động trong ứng dụng phải được bảo đảm kỹ lưỡng. Các thử nghiệm trong phần này đảm bảo rằng "logic" của ứng dụng thể bị thay đổi (như không thể kích hoạt bước sau khi chưa hoàn tất bước trước)
	Kiểm tra xử lý phía người dùng	Các bài kiểm tra được thiết kế trong phần này để xác định là nếu thông tin nhạy cảm có thể được tìm thấy trong mã HTML của các ứng dụng, và mặt khác, khả năng thay đổi các dữ liệu này trái với quy tắc của ứng dụng sẽ không được chấp nhận bởi các ứng dụng để đảm bảo tính bảo mật và tính toàn vẹn.
2.2	**Báo cáo**	Tất cả các kết quả kiểm tra, bằng chứng lỗ hổng, phương pháp chứng minh các lỗ hổng bảo mật đều phải được ghi nhận một cách chi tiết và đầy đủ. Báo cáo phải rõ ràng, ngắn gọn và được tổ chức tốt, cho phép các bên liên quan hiểu được tình hình bảo mật và thực hiện các hành động thích hợp để giải quyết các rủi ro đã xác định.
2.3	**Hỗ trợ kỹ thuật**	Đội ngũ kỹ sư đánh giá bảo mật sẽ phối hợp cùng đội ngũ cán bộ kỹ thuật của đơn vị để tư vấn các phương án xử lý lỗ hổng bảo mật, cập nhật bản vá. Sau quá trình xử lý lỗ hổng, các kỹ sư hỗ trợ xác minh, đánh giá lại trạng thái của các lỗ hổng bảo mật đã được phát hiện trước đó.
3	**Kiểm tra, rà soát bảo mật cho các thiết bị mạng, thiết bị bảo mật**	
3.1	**Tiêu chuẩn đánh giá**	Việc kiểm tra được thực hiện dựa trên Luật An toàn thông tin mạng 2015 đối với các thiết bị mạng, thiết bị bảo mật.
	Lên kịch bản, các phương án đánh giá	Xác định và thống nhất thành phần cần thực hiện kiểm tra, các hướng tiếp cận ứng với từng phạm vi cụ thể, lập kế hoạch dò quét và kiểm tra. Chuẩn bị các tài nguyên, công cụ cần thiết ứng với các mục tiêu trong phạm vi kiểm tra.
	Thu thập thông tin	Thu thập thông tin là giai đoạn đầu tiên trong quá trình kiểm tra đánh giá mà ở đó các kỹ sư của nhà cung cấp sẽ cố gắng thu thập nhiều nhất có thể các thông tin về mục tiêu để hỗ trợ cho công việc tìm kiếm và khai thác lỗ hổng bảo mật sau này. Ở một mức độ rộng nhất trong phạm vi kiểm tra đánh giá thông tin này sẽ bao gồm thông tin về nhân viên, cơ sở vật chất, các sản phẩm và kế hoạch, các thông tin bí mật, riêng tư hoặc tất cả các thông tin liên quan đến mục tiêu.
	Phân tích, nhận dạng điểm yếu	Phân tích lỗ hổng bảo mật được sử dụng để đánh giá các rủi ro xảy ra đối với các lỗ hổng bảo mật tồn tại. Công việc phân tích lỗ hổng bảo mật được chia làm 2 phần. Nhận dạng lỗ hổng bảo mật và xác nhận lại sự tồn tại của lỗ hổng trên hệ thống. Nỗ lực tìm kiếm lỗ hổng bảo là công việc chính trong giai đoạn nhận dạng lỗ

		hổng. Xác nhận lại sự tồn tại của lỗ hổng sẽ làm giảm số lượng các lỗ hổng trong phần nhận dạng và chỉ giữ lại các lỗ hổng nào thực sự hợp lệ. Thu thập thông tin CVE trên hệ thống, thực hiện kiểm tra khả năng khai thác của các CVE này.
3.2	**Báo cáo**	Tất cả các kết quả kiểm tra, bằng chứng lỗ hổng, phương pháp chứng minh các lỗ hổng bảo mật đều phải được ghi nhận một cách chi tiết và đầy đủ. Báo cáo phải rõ ràng, ngắn gọn và được tổ chức tốt, cho phép các bên liên quan hiểu được tình hình bảo mật và thực hiện các hành động thích hợp để giải quyết các rủi ro đã xác định.
3.3	**Hỗ trợ kỹ thuật**	Đội ngũ kỹ sư đánh giá bảo mật sẽ phối hợp cùng đội ngũ cán bộ kỹ thuật của đơn vị để tư vấn các phương án xử lý lỗ hổng bảo mật, cập nhật bản vá. Sau quá trình xử lý lỗ hổng, các kỹ sư hỗ trợ xác minh, đánh giá lại trạng lại của các lỗ hổng bảo mật đã được phát hiện trước đó.
II	**Kiểm tra tiêu chuẩn cấu hình an toàn**	
	Kiểm tra tiêu chuẩn cấu hình an toàn cho các máy chủ, máy trạm, CSDL, ứng dụng Web, thiết bị bảo mật… tuân theo tiêu chuẩn CIS Benchmarks, đồng thời tham chiếu đến các tài liệu cấu hình bảo mật tiêu chuẩn của các công nghệ liên quan.	
1	**Kiểm tra tiêu chuẩn cấu hình an toàn cho nền tảng, hệ điều hành**	
	Kiểm tra các bảng cập nhật, vá lỗi và các phần mềm bảo mật.	
	Kiểm tra cấu hình tập tin hệ thống (Ext3, NTFS).	
	Kiểm tra các dịch vụ hệ điều hành.	
	Kiểm tra các dịch vụ đặc biệt.	
	Kiểm tra log và các dịch vụ theo dõi sự kiện hệ thống (auditing services).	
	Kiểm tra cấu hình mạng và tường lửa.	
	Kiểm tra vấn đề phân quyền truy cập hệ thống, xác thực.	
	Kiểm tra các tài khoản và các môi trường.	
	Kiểm tra các cấu hình cảnh báo về quyền.	
	Kiểm tra các vấn đề bảo trì, cập nhật hệ thống.	
2	**Kiểm tra tiêu chuẩn cấu hình an toàn cho cơ sở dữ liệu**	
	Kiểm tra phiên bản nền tảng, hệ điều hành đang triển khai cơ sở dữ liệu	
	Kiểm tra phân quyền tập tin hệ thống lưu trữ dữ liệu	
	Kiểm tra các cài đặt nhật ký (Logging)	
	Kiểm tra các vấn đề chung liên quan đến cơ sở dữ liệu	
	Kiểm tra quyền truy cập trên các cơ sở dữ liệu	
	Kiểm tra các cấu hình tùy chỉnh	
	Kiểm tra các cấu hình liên quan mã hoá	
	Kiểm tra các cấu hình sao lưu và phục hồi sau thảm họa.	
3	**Kiểm tra tiêu chuẩn cấu hình an toàn cho máy chủ ứng dụng, máy chủ Web**	
	Kiểm tra phiên bản của máy chủ ứng dụng	
	Kiểm tra các tuỳ chọn trong quá trình cài đặt máy chủ ứng dụng	
	Kiểm tra cấu hình hệ điều hành đang triển khai máy chủ ứng dụng	

	Kiểm tra quản lý truy cập, phân quyền người dùng cho các tiến trình của ứng dụng
	Kiểm tra các cấu hình bảo mật trên thư mục lưu trữ mã nguồn, dữ liệu
	Kiểm tra các cấu hình xác thực
	Kiểm tra các cấu hình các giải pháp mã hoá như SSL/TLS
	Kiểm tra các cấu hình ghi nhận nhật ký (Logging)
	Kiểm tra các cấu hình sao lưu hệ thống
	Kiểm tra các cấu hình truy cập từ xa và cập nhật nội dung mã nguồn.
4	**Kiểm tra tiêu chuẩn cấu hình an toàn cho thiết bị mạng, thiết bị bảo mật**
	Kiểm tra phiên bản, các bản cập nhật của Firmware/Software
	Kiểm tra các yêu cầu truy cập trên thiết bị (AAA, AccNCC rule, Banner rule, Password…).
	Kiểm tra các phân quyền truy cập vào cổng quản trị
	Kiểm tra các cấu hình ghi nhận nhật ký (Logging), giám sát thiết bị
	Kiểm tra các yêu cầu truyền dẫn dữ liệu (Border routing, Neighbor authentication, Routing rule, Firewall rule….)
	Kiểm tra các cấu hình sao lưu, khôi phục hệ thống
	Kiểm tra các cấu hình mã hoá, giải mã

PHỤ LỤC 04
BẢNG GIÁ DỊCH VỤ

STT	Nội dung	Thành tiền (VNĐ)
I	**Dịch vụ tư vấn kỹ thuật và đánh giá an toàn thông tin**	
1	**Tư vấn và hỗ trợ trong quá trình thiết kế giải pháp và tích hợp dịch vụ:** 1. Tư vấn xây dựng luồng nghiệp vụ giải pháp 2. Tư vấn xây dựng mô hình kiến trúc hạ tầng 3. Hỗ trợ chuẩn bị tài liệu thông tin cấu hình, tài khoản dev/test 4. Hỗ trợ trong quá trình khách hàng tích hợp SDK, tích hợp API với TTXT	
2	**Tư vấn và hỗ trợ hoàn thiện hồ sơ, thủ tục:** 1. Hỗ trợ chuẩn bị hồ sơ đăng ký khai thác dịch vụ xác thực điện tử 2. Hỗ trợ xây dựng kịch bản nghiệm thu trên môi trường UAT và Production 3. Hỗ trợ chuẩn bị, hoàn thiện hợp đồng khai thác dịch vụ các các phụ lục liên quan 4. Hỗ trợ thúc đẩy quá trình ký hợp đồng và xin cấp phép kết nối dịch vụ	
3	**Đánh giá an toàn thông tin, tư vấn, hỗ trợ trong quá trình triển khai, nâng cấp các phương án an toàn thông tin** 1. Khảo sát và thu thập thông tin 2. Xây dựng phương án đánh giá 3. Thực hiện đánh giá theo kịch bản 4. Tổng hợp và báo cáo 5. Hỗ trợ kỹ thuật 6. Rà soát và đánh giá lại 7. Hoàn thiện báo cáo cuối cùng 8. Hỗ trợ trong giai đoạn C06 kiểm tra	
II	**Dịch vụ thuê hạ tầng giải pháp và dịch vụ đảm bảo ANAT bao gồm:** Thiết bị máy chủ Agent GW và Thiết bị Cân bằng tải và các giải pháp bảo đảm ANAT hệ thống (WAF, NGFW, Phần mềm giám sát hạ tầng (Hiệu năng, CPU, RAM,...) và giám sát ATTT.	
III	**Cung cấp thiết bị:** HSM Thales A750 1. Số lượng: 02 thiết bị 2. Thông số kỹ thuật: - RSA - 2048 signing ops: 5000 - ECC P256 signing ops: 10000 - AES - GCM small packet encryption ops: 10000 3. Dịch vụ triển khai và hỗ trợ kỹ thuật 1 năm	